Version 1.0 | 14-3-2018

Security assessment of Dutch election software OSV P4 and P5

Public

Sijmen Ruwhof

IT Security Researcher / Ethical Hacker
sijmen@ruwhof.net
https://sijmen.ruwhof.net

Management summary

In February 2018 an independent security assessment was started on the software that totalize votes in the upcoming Dutch elections on March 21, 2018. The software is called OSV (Ondersteunende Software Verkiezingen) and made by German company IVU Traffic Technologies AG. IVU was hired to do so by the Electoral Council (Kiesraad).

This independent research was voluntary conducted by IT security researcher and ethical hacker Sijmen Ruwhof[1], in close collaboration with investigative journalist Bart van de Berg from RTL News. This report is the result of that research. The following IT security experts also collaborated with validating findings and where consulted:

1. Election security specialists Rob Gonggrijp and Arjen Kamphuis.
2. Professor IT security Herbert Bos from VU University Amsterdam.
3. Independent IT security researchers and ethical hackers Ger Schinkel and John de Kroon.

OSV should be able to withstand advanced attacks

The Electoral Council has expressed the ambition that the OSV vote count software should be able to withstand advanced and persistant attacks, such as foreign intelligence agencies that want to attack our democracy and manipulate votes. Compromising OSV should not lead to be able to manipulate votes.[2] In short: OSV must withstand all attacks by even the best hackers in the world.

Major notable events in last years election

One year ago in January 2017 OSV was also independently researched for vulnerabilities by Sijmen Ruwhof and RTL News. That security research was published by RTL News on Dutch national Tv on January 30, 2017. It proved that the Dutch elections in March 2017 could be easily hacked. That research raised a lot of media attention. Because of that, Dutch minister Plasterk of Internal Affairs mandated that municipalities should manually totalize all vote totals on level of political party. OSV was not allowed to be used for this anymore. This was a major improvement in making the election much more hacker proof.

Cyber security firm Fox IT was hired by the Electoral Council to investigate OSV security and processes around it. They released their security report on March 3, 2017 and confirmed all major findings that were already published on January 30, 2017. Fox IT also found more severe vulnerabilities.[3]

On December 15, 2017 the Electoral Council published a follow-up report on the security improvements made in OSV based on Fox IT's report. The Electoral Council and municipalities believe that OSV is secure again to be used and trusted again in the 2018 election.

[1] Weblog of Sijmen Ruwhof: https://sijmen.ruwhof.net/ LinkedIn profile: https://linkedin.com/in/sruwhof

[2] See page 4 in the Fox IT report published on March 3, 2017: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2017/03/02/rapport-%CB%9Donderzoek-osv-en-proces-rapportage%CB%9D/rapport-%CB%9Donderzoek-osv-en-proces-rapportage%CB%9D.pdf

[3] See website address in above footnote for the Fox IT report.

Scope of investigation

OSV program 4 and 5 (P4, P5) version 2.21.4 was in scope and researched in this security assessment. This is the official version that will be used in the Dutch elections that will be held on March 21, 2018[4]. OSV P4 and P5 are responsible for totalizing the election outcome.

For this security assessment limited time was available. This means that not all security vulnerabilities could be identified in OSV and processes around it. If more time was available, (much) more security vulnerabilities could probably be identified. It is however believed that this security research gives enough insight into the security status of the OSV P4 and P5 and the safety of the upcoming elections at this point.

Overview of security risks found in OSV

After completing the security review of OSV P4 and P5 and the processes around it, 47 security vulnerabilities were found in OSV and processes around it:

Total findings	Risk
1	Critical
9	High
25	Medium
9	Low
3	Very low
5	Remarks

Most important findings

1. **Software decides who won the election and this output is fully trusted again**
   RTL News found out that the Electoral Council and municipalities silently trusted OSV output again and will use it to calculate who will win the upcoming elections on March 21, 2018. This renewed trust in OSV was not validated by an independent respectable cyber security firm. The Electoral Council did not hire Fox IT again in 2018 to check if all major security risks were properly solved in the new OSV version made by IVU.

   After election day on March 22, 2018, civil servants from the central vote office of a municipality will enter vote totals from polling stations into OSV (see chapter 4.1.1). OSV will totalize all vote totals per candidate and generate a PDF file that contains the election result that has to be printed (a N11 and O3 document). The printed election result becomes official and trusted 'paper that is in the lead'. It will not be manually validated by civil servants as OSV is trusted to be unhackable again.

   If someone hacks the OSV server, then this person can easily manipulate votes by changing votes stored in the OSV database and in the PDF files stored on the server that have to be printed.

[4] See: https://www.kiesraad.nl/verkiezingen/gemeenteraden/ondersteunende-software-verkiezingen-osv/osv-voor-gemeenten

2. **OSV security has not been substantially improved in comparison with last year**
   If OSV output is trusted again, you would expect security to be significantly improved. And indeed, security improvements have been made. However, not enough. Last year on January 30, 2017 IT security researcher Sijmen Ruwhof published on his weblog a detailed technical analysis of all the weaknesses he found in OSV P4 and P5.[5] A retest has been performed to see if the findings mentioned on the weblog were resolved in the latest version of OSV:

Status	Total findings
Total vulnerabilities unsolved	**16**
Total vulnerabilities partly solved	**9**
Total vulnerabilities solved	**8**

   There are 25 open security risks after the retest (all unsolved and partly solved findings):

Total findings	Risk
1	**Critical**
4	**High**
18	**Medium**
1	**Low**
1	**Very low**

   The retest shows that OSV security has not been substantially improved in comparison with last year (see chapter 3).

3. **OSV uses out-dated, deprecated and insecure technology from ten years ago**
   OSV has been developed in 2008 and has not changed a lot over the years. The OSV version used in the March 2018 election still uses very old and insecure (JBoss & Java) technology from 2008 and 2013, that misses many important security updates (see chapter 4.1.4). These technologies are also not properly configured and hardened against hack attacks (see chapter 4.1.3 and 4.1.5). An advanced hacker that has gained access to the offline OSV network of a municipality could break into the OSV server by exploiting unpatched security vulnerabilities. Once an adversary has gained access to the OSV server, votes can be easily changed without detection (see chapter 4.1.2).

   Professor IT security Herbert Bos from VU University Amsterdam also independently investigated the OSV source code. He came to the following conclusion: *"The OSV source code is written very poorly. For that reason alone it should be abolished."*

4. **Sophisticated or opportunistic attackers can influence election outcome probably unnoticed**
   Based on the all the 47 vulnerabilities found in OSV and processes around it, it is believed that hackers from foreign intelligence agencies can easily manipulate vote totals by hacking into the OSV server of a municipality. But election fraud may also come from much closer, for example from opportunistic or bribed system administrators working at municipalities that already have full access over the OSV server (see chapter 2.1.2 and 4.1.2). As active security and fraude monitoring on OSV servers is missing (see chapter 4.1.2, 4.1.8, 4.1.10 and 4.1.18), fraud will probably go undetected if done not too obviously and greedy.

[5] See: https://sijmen.ruwhof.net/weblog/1166-how-to-hack-the-upcoming-dutch-elections

5. **Official vote reports from polling stations are not published on the internet**
   Currently it is up to each municipality to publish the vote totals of each polling station on their website. Some cities publish in their own format all the vote totals of a polling station, and others only publish the aggregated total votes in a municipality without details of all the vote totals of each polling station. Scans of each official paper polling station report (process-verbaal) are never uploaded to the internet. A digital export file of all the vote totals is generated by OSV. This file is in some cases converted to HTML by municipalities and published (partially) on their website.

   The official polling station reports that contain all the vote totals of a municipality can only be looked at offline at the office of a municipality. This raises the bar significantly for citizens and polling station chairmans to validate if someone has tampered with the election outcome in the totalization process. If a concerned citizen wants to independently validate all the totalizing of votes himself in The Netherlands, he or she would have to visit each municipality and copy all the official reports from polling stations. This takes a lot of time. Elections should be completely verifiable with minimal effort by everyone that thinks election integrity is at risk.

Most important recommendations

1. **Do not trust output from OSV again: use OSV to validate manually counted votes**
   History shows that exclusive manual aggregation of vote totals is error-prone[6], and exclusive digital aggregation of vote totals is vulnerable to manipulation by sophisticated attackers[7].

   OSV can be useful however, even to strengthen the security of an election. All vote totals for each candidate from a political party should be manually totalized by the central vote office of a municipality. Afterwards, the vote totals as calculated by each independent polling station in a municipality should be entered into OSV. OSV should also totalize all vote totals and calculate who won the election. OSV output should be used to verify if the manual totalization is done properly and without mistakes.

   Untrusting OSV and manually totalizing vote totals takes a couple more days to perform, but eliminates all the risks that our election can be hacked by manipulating vote totals. Waiting a couple more days on the election outcome is nothing compared to the impact if the election gets hacked. Official paper vote total reports of municipalities should be manually be filled in by civil servants based on the manual calculated vote totals. OSV prints should never be used as official documents anymore. The cyber security of OSV is of much less importance if its output is distrusted.

2. **Complete transparency and easy access of official vote reports from polling stations**
   It is strongly advised to immediately scan all official vote total reports (processen-verbalen) from polling stations and upload them to a secure portal a couple of days after elections are held. This portal does not currently exist and should be developed by the Central Electoral council. This portal should also also publish all uploaded official vote totals reports on their website so people can independently review them.

   In a reaction the Electoral Council states towards RTL News that: *"A bill is being prepared in which all official reports from polling stations will be made public on the internet in the future."*. Good to hear this point is already being picked up!

[6] See news story from June 13, 2017: https://www.trouw.nl/home/veel-stemmen-verkeerd-geteld-bij-kamerverkiezingen~ab6e2a02/
See news story from March 28, 2017: https://www.rtlnieuws.nl/nederland/politiek/van-alles-misgegaan-bij-optellen-stemmen-verkiezingen

[7] As proven by RTL News and Sijmen Ruwhof on January 30, 2017 and by Fox IT in their report published on March 3, 2017.

Conclusion

It is strongly and urgely recommended to not trust software output in determinting who won an election. Software can be hacked undetectable on many level and stages. Even offline and air-gapped networks can be hacked with utmost precision, as shown in the news about the Stuxnet worm in 2010[8]. Recent history has shown that intelligence agencies worldwide have breached the most well protected IT networks in the world with highly advanced and complex malware infrastructure.

OSV uses out-dated, deprecated and insecure technology from ten years ago. OSV security has not been substancially improved in comparison with last year. It is build by a software company that seem to have no clue about how to protect software against hackers and the cyber threat landscape of nowadays. Over 50 security weaknesses have been identified in only a couple of days. OSV's security architecture is broken by design: it has major security flaws that can't be fixed.

OSV should be used only to validate if manual totalizing vote totals is done properly and without any mistakes.

[8] See: https://en.wikipedia.org/wiki/Stuxnet

Table of contents

1 Introduction

In February 2018 an independent security assessment was started on the software that totalize votes in the upcoming Dutch elections on March 21, 2018. The software is called OSV (Ondersteunende Software Verkiezingen) and made by German company IVU Traffic Technologies AG. IVU was hired to do so by the Electoral Council (Kiesraad).

This independent research was voluntary conducted by IT security researcher and ethical hacker Sijmen Ruwhof[9], in close collaboration with investigative journalist Bart van de Berg from RTL News. This report is the result of that research. The following IT security experts also collaborated with validating findings and where consulted:

1. Election security specialists Rob Gonggrijp and Arjen Kamphuis.
2. Professor IT security Herbert Bos from VU University Amsterdam and his team.
3. Independent IT security researchers and ethical hackers Ger Schinkel and John de Kroon.

1.1 OSV should be able to withstand advanced attacks

The Electoral Council has expressed the ambition that the OSV vote count software should be able to withstand advanced and persistent attacks, such as foreign intelligence agencies that want to attack our democracy and manipulate votes. Compromising OSV should not lead to be able to manipulate votes. In short: OSV must withstand all attacks by even the best hackers in the world.

1.2 Major notable events in last years election

One year ago (January 2017) OSV was also independently researched for vulnerabilities by Sijmen Ruwhof and RTL News. That security research was published by RTL News on Dutch national Tv on January 30, 2017. It proved that the Dutch elections in March 2017 could be easily hacked. That research raised a lot of media attention. Because of that, Dutch minister Plasterk of Internal Affairs mandated that municipalities should manually totalize all vote totals on level of political party. OSV was not allowed to be used for this anymore. This was a major improvement in making the election much more hacker proof.

Cyber security firm Fox IT was hired by the Electoral Council to investigate OSV security and processes around it. They released their security report on March 3, 2017 and confirmed all major findings that were already published on January 30, 2017. Fox IT also found more severe vulnerabilities.[10]

On December 15, 2017 the Electoral Council published a follow-up report on the security improvements made in OSV based on Fox IT's report. The Electoral Council and municipalities believe that OSV is secure again to be used and trusted again in the 2018 election.

[9] Weblog of Sijmen Ruwhof: https://sijmen.ruwhof.net/ LinkedIn profile: https://linkedin.com/in/sruwhof

[10] See website address in above footnote for the Fox IT report.

Date	Title	Authors
January 30, 2017	How to hack the upcoming Dutch elections – and how hackers could have hacked all Dutch elections since 2009	Sijmen Ruwhof
January 30, 2017	Met potlood stemmen onveilig: verkiezingsuitslag eenvoudig te hacken	*RTL News:* Bart van den Berg, Daniël Verlaan
January 30, 2017	Zo werkt het softwaresysteem dat onze stemmen telt	*RTL News:* Bart van den Berg, Daniël Verlaan
February 1, 2017	Vrees voor hackers: kabinet schrapt software, stemmen tellen volledig met de hand	*RTL News:* Bart van den Berg, Daniël Verlaan, Siebe Sietsma.
March 3, 2017	Onderzoek OSV en proces rapportage	*Fox IT:* Paul Pols, Daniël Niggebrugge, Francisco Dominguez
December 15, 2017	Follow-up bevindingen Fox IT en aanpassingen OSV gemeenteraadsverkiezingen en raadgevend-referendum 2018	Kiesraad
February 5, 2018	Toetsingsrapport SQS OSV programma 4 en 5	SQS

1.3 Motivation behind research

Democratic elections are one of the most important processes in a country. They should be very reliable, trustworthy and secure. Unfortunately, history has shown that the Dutch elections could be easily hacked since the introduction of electronic voting machines by municipalities.

Hacking was never seen as a real threat by the municipalities and the Electoral Council. Only the positive sides of IT were seen: computers don't make mistakes and manually counting is messy and prone to human counting mistakes. Speeding up the vote totalizing process seems to be the primary concern of municipalities and the Electoral Council. There is a lot of political pressure to get the election results as fast as possible.

Action group We Don't Trust Voting Machines proved in 2006 that Dutch voting machines could be easily hacked. In 2006 and 2007 voting machines were banned from usage after it was proven that these were very insecure. Solid pen and paper is used since these years.

The Electoral Council hired German company IVU in 2008 to develop vote total processing software that municipalities could use. Since 2009 pen and paper is used during election day in the front-office, and quietly OSV software was used in the back-office. OSV calculated who won the elections from 2009 till 2017. OSV output was not validated as it was completely trusted. OSV saved a lot of manually work for municipalities, so it was very welcomed there.

Nobody outside the municipalities, Electoral Council and the ministry of Internal Affairs seemed to know, or to be aware about the existence of OSV and the crucial role it played in the background. After it was proved on January 30, 2017 that OSV could also be easily hacked, the Electoral Council and municipalities blindly dismissed the findings and were angry about the raised security concerns. They wanted OSV back because it saved them lots of extra manual counting work. Luckily OSV was forbidden by the minister of Internal Affairs. The Netherlands had tamper proof elections again on March 15, 2017, because OSV output was not trusted anymore to determine which political parties won the election.

All Dutch elections held since 2009 could be easily hacked. It is unknown if someone has hacked an election, as most evidence must be removed by law after 3 months after an election is held (see chapter 2.2). There has never been performed a forensic investigation if an OSV server has been hacked. OSV has always been assumed to be secure and hacking was never seen as a real threat.

After the 2017 elections, the Electoral Council processed the Fox IT report and released a new OSV version on in February 2018 that should be secure again. OSV output will be trusted again in the upcoming elections. The main question arose immediately if OSV could be easily hacked again, and thus this investigation was started.

1.4 Scope

OSV program 4 and 5 (P4, P5) version 2.21.4 was in scope and researched in this security assessment. This is the official version that will be used in the Dutch elections that will be held on March 21, 2018[11]. OSV P4 and P5 are responsible for totalizing the election outcome.

Other relevant components that play an important role in the Dutch elections, but are not researched (in-depth):

- OSV program 1, 2 and 3.
- Source code of OSV P4 and P5.[12]
- Infrastructure municipalities use to run OSV locally on.
- The laptop the Electoral Council uses to run OSV on to determine the referendum outcome.
- The computers the 20 Election Districts use to process the referendum outcome on.
- The Stembureau-app.
- The website www.kiesraad.nl.
- Internet-facing IVU infrastructure: `91.212.245.0/24`.

For this security assessment limited time was available. This means that not all security vulnerabilities could be identified in OSV and processes around it. If more time is available, (much) more security vulnerabilities could probably be identified. It is however believed that this security research gives enough insight into the security status of the OSV P4 and P5 and the upcoming elections at this point.

[11] See: https://www.kiesraad.nl/verkiezingen/gemeenteraden/ondersteunende-software-verkiezingen-osv/osv-voor-gemeenten

[12] See: https://www.kiesraad.nl/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/osv-broncode-programma-4-en-5-versie-2.21.4

1.5 Timeline

Date	Title
February 13, 2018	Electoral Council sent OSV P4 and P5 on CD-ROM by post to RTL News research redaction.
February 22, 2018	RTL News sent the CD-ROM file to Sijmen Ruwhof and the security assessment started.
March 12, 2018	RTL News notified the Electoral Council about the vulnerabilities found and asked for a reaction before publication.
March 13, 2018	This security assessment of OSV is published via Dutch national Tv by RTL News.

1.6 Authenticity of tested software

As the OSV P4 and P5 software is not downloadable from www.kiesraad.nl, the RTL News research department asked the Electoral Council to send them a copy of P4 and P5 so they could let someone inspect it. The Electoral Council sent on February 13, 2018 OSV P4 version 2.21.4 on CD-ROM to RTL News. The CD-ROM was accompanied with documentation on paper that was also sent to ICT department at municipalities. The contents of the received CD-ROM and OSV documentation were researched in this security assessment.

2 Election fraud hacking threat model

The Fox IT security report from 2017 about OSV states the following about recent development in election fraud that has been discovered in other countries[13]:

- *"[..] De Kiesraad heeft de ambitie uitgesproken dat het vaststellen van de verkiezingsuitslag weerbaar moet zijn tegen aanvallen van dergelijke [statelijke, red.] actoren. Derhalve behoort ernaar gestreefd te worden dat het compromitteren van OSV op enig moment in de procesketen er niet toe zou mogen leiden dat de verkiezingsuitslag ongemerkt gemanipuleerd kan worden. [..]*

  Inzicht in het dreigingsbeeld dat van toepassing is op (het gebruik van) OSV kan worden verkregen via publiek beschikbare informatie met betrekking tot aanvallen die zijn gericht op verkiezingen of die hieraan gerelateerd zijn. Het meest relevante publiek bekende incident is de aanval van "CyberBerkut" op de Central Election Commission (CEC) van Oekraïne gedurende de presidentsverkiezingen in mei 2014. Als gevolg van de aanval werden delen van de infrastructuur, die bedoeld was om real-time updates te tonen van stemaantallen, onbeschikbaar gemaakt. Enkele minuten voordat de stembureaus sloten, werd door de aanvallers ook een foto van één van de kandidaten geplaatst op de website van de CEC, waarin abusievelijk werd vermeld dat de betreffende kandidaat de verkiezingen zou hebben gewonnen, hetgeen direct werd overgenomen door Russische nieuwsstations (NATO CCD COE Publications, 2015).

  Bij het onderzoek naar de CyberBerkut hack is door CERT-UA de Sofacy/Sednit/APT28-malware aangetroffen in het CEC-netwerk (NATO CCD COE Publications, 2015, p. 57). Deze malware wordt in verband gebracht met geavanceerde aanvallen die zouden zijn uitgevoerd door de Russische actor "Fancy Bear" (FireEye, 2014). Het formele stemproces in de Oekraïne was ten tijde van de aanval naar verluidt exclusief gebaseerd op papier en een handmatige verificatie daarvan. Desalniettemin kan een dergelijke aanval de legitimiteit van het verkiezingsproces in de ogen van (bepaalde groepen) burgers schaden, wat derhalve ook het primaire oogmerk kan zijn van een aanvaller (NATO CCD COE Publications, 2015).

  In januari van dit jaar is de hack van het Democratische Nationale Comité (DNC) in de Verenigde Staten door de CIA, FBI en NSA publiekelijk geattribueerd aan de Russische militaire inlichtingendienst (General Staff Main Intelligence Directorate). Gezamenlijk hebben deze diensten met een hoge mate van vertrouwen geconcludeerd dat de DNC-hack onderdeel uitmaakte van een bredere campagne om het publieke vertrouwen in het democratische proces in de Verenigde Staten te ondermijnen. Deze campagne was gebaseerd op een strategie waarin geheime inlichtingenoperaties werden vermengd met openlijke inspanningen door Russische overheidsdiensten, staatsmedia en derden zoals betaalde sociale media gebruikers (Office of the Director of National Intelligence, 2017).

  Gevraagd naar de attributie aan Rusland van de DNC-hack heeft president Obama gesteld dat "on a regular basis, they try to influence elections in Europe" (New York Times, 2016). Deze informatie is indicatief dat aanvallers potentieel belang kunnen hebben bij het verstoren of anderszins beïnvloedden van (de gepercipieerde legitimiteit van) het verkiezingsproces in Nederland. Actoren van vermoedelijk Russische oorsprong zijn niet de enige actoren die belang kunnen hebben bij het verkrijgen van inzicht in of zelfs het beïnvloedden van (de gepercipieerde legitimiteit van) verkiezingen in andere landen.

[13] See page 4: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2017/03/02/rapport-%CB%9Donderzoek-osv-en-proces-rapportage%CB%9D/rapport-%CB%9Donderzoek-osv-en-proces-rapportage%CB%9D.pdf

> *Tussen 1960 en 2006 zou in meer dan 120 nationale verkiezingen in 66 landen gepoogd zijn de uitkomst van de verkiezingen te beïnvloedden door buitenlandse mogendheden (Corstange, 2012). De relatief recente opkomst en prevalentie van digitale hulpmiddelen, die hierin op enigerlei wijze een rol kunnen spelen, biedt aanvallers in dat kader een veelvoud aan mogelijkheden. Daarnaast toont de publiek beschikbare informatie aan dat andere actoren in context van democratische verkiezingen een doelwit kunnen zijn, waaronder individuele politieke partijen of kandidaten (inclusief hun privésfeer), zoals ook is gebleken in de aanloop naar de Amerikaanse presidentsverkiezingen in 2016. Verder kan onzorgvuldige berichtgeving door media, bijvoorbeeld op basis van een onvolledig beeld of onjuiste informatie, de gepercipieerde legitimiteit van democratische verkiezingen (abusievelijk) negatief beïnvloedden.*
>
> *Gegeven het geschetste dreigingsbeeld en belang van de integriteit van de formele verkiezingsuitslag is het aan te raden om de assume breach en defense in depth principes toe te passen. Uit het assume breach principe volgt dat rekening gehouden moet worden met de mogelijkheid dat één of meerdere willekeurige componenten op enig moment gecompromitteerd kunnen worden. Defense in depth houdt in dat, zelfs indien één of meer componenten gecompromitteerd worden, het proces van het aggregeren van de stemmen voldoende weerbaar is tegen aanvallen door aanvullende technische of procedurele maatregelen. Dit kunnen aanvullende preventieve maatregelen zijn, maar het kunnen nadrukkelijk ook aanvullende detectieve en responsieve maatregelen betreffen.*
>
> *Uit het dreigingsbeeld dat van toepassing is op (het gebruik van) OSV blijkt dat rekening moet worden gehouden met statelijke actoren die belang kunnen hebben bij het verstoren of anderszins beïnvloedden van (de gepercipieerde legitimiteit van) het democratische verkiezingsproces in Nederland. Gegeven het belang van de integriteit van het verkiezingsproces zou ernaar gestreefd behoren te worden dat het compromitteren van systemen van individuele stembureaus (PSB, HSB, CSB) er niet toe zou mogen leiden dat de verkiezingsuitslag ongemerkt beïnvloed zou kunnen worden.”*

2.1 Threat actors

Some of the threat actors that might want to influence the upcoming elections:

1. Foreign intelligence agencies that want to gain political influence in The Netherlands.
2. Candidates that want to run for office in their own municipality.
3. Drugs criminals that want to gain access to the local council.
4. Opportunistic or bribed system administrators or OSV end-users at municipalities.
5. All personnel that has access to air-gapped OSV network
6. Political activists.
7. Cyber terrorists that want to disrupt the trust in the Dutch elections by obviously manipulating election results.

2.1.1 Foreign intelligence agencies

The Fox IT security report from 2017 about OSV states[14]:

- *"[..] Uit de analyse van het dreigingsbeeld dat van toepassing is voor (het gebruik van) OSV, blijkt dat rekening gehouden moet worden met statelijke actoren die belang kunnen hebben bij het beïnvloeden van (de gepercipieerde legitimiteit) van het democratische verkiezingsproces in Nederland. [..] [..]"*

Some of the reason why foreign intelligence agencies might want to influence the upcoming elections could be:

1. Influencing the referendum that will be held. The referendum will be held about if it is a good idea that the Dutch intelligence agencies are allowed to intercept wired data traffic (also called the drag law by opponents). Dutch intelligence agencies have acquired this new power recently. Big internet cables from overseas enter Europe via Amsterdam. Dutch intelligence agencies are now allowed to intercept traffic from these cables in certain scenario's. This is not good news for foreign hostile countries. Their traffic will also be intercepted and analysed in the future.
2. Get political influence in major Dutch cities such as Amsterdam, Den Haag, Rotterdam and Utrecht. These cities alone have around 2.4 million inhabitants in total[15]. That is 14% of the Dutch population[16].

2.1.2 Opportunistic or bribed system administrators or OSV end-users at municipalities

System administrators at municipalities have full control over the local OSV network and computers. They need this kind of access to install the OSV server and setup the network. There is no four-eyed procedure implemented here. They can easily install software on the OSV server that manipulates the OSV database on the server after users have entered votes into the database. This fraud can go unnoticed as OSV output is trusted after two people have entered the vote totals in the system. After the attack the system administrator can wipe all his traces.

Opportunistic or bribed OSV end-users
OSV end-users that have to fill in vote totals in OSV have physical access to the OSV network and connected devices. They could install hardware keyloggers to gain access to the other OSV users, such as the administrator account of OSV. They could also connect a SIM card enabled hardware device with 3G/4G connection to the offline OSV network to connect the network to the internet. With access to the OSV network they could also exploit unpatched software vulnerabilities in the OSV server to gain access to it.

Actual case of insider threat in 2008
In 2008 a man was sentenced by court in The Netherlands for election fraud in 2006 with a voting computer in the municipality of Landerd in the municipal elections[17]. The manipulation was done very obviously and could therefor be easily detected.

[14] See page 4: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2017/03/02/rapport-%CB%9Donderzoek-osv-en-proces-rapportage%CB%9D/rapport-%CB%9Donderzoek-osv-en-proces-rapportage%CB%9D.pdf

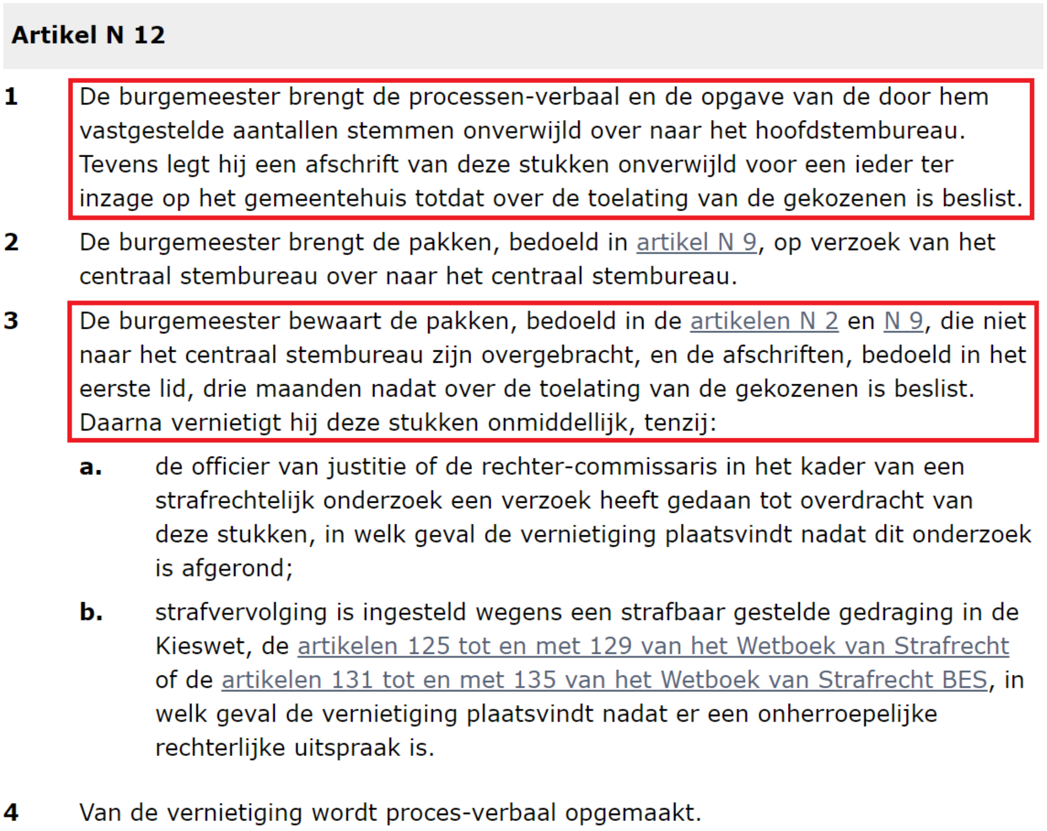
[15] 2,363,722 inhabitants to be exactly, see: https://nl.wikipedia.org/wiki/Lijst_van_grootste_gemeenten_in_Nederland

[16] Total estimated inhabitants by CBS in The Netherlands is 17,203,411 on February 20, 2018, see https://www.cbs.nl/nl-nl/visualisaties/bevolkingsteller

[17] See: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHSHE:2008:BC2171

2.2 Hackers can only be catched until 3 months after an election

According to Dutch law[18], evidence of an election has to be destroyed three months after it was held. Election fraud can therefor only be properly detected until three months after an election. Afterwards, all paper votes and all the official paper vote reports must be deleted. Most companies take over six months to detect a data breach[19]. The time-frame to catch hackers is very short.



Artikel N 12

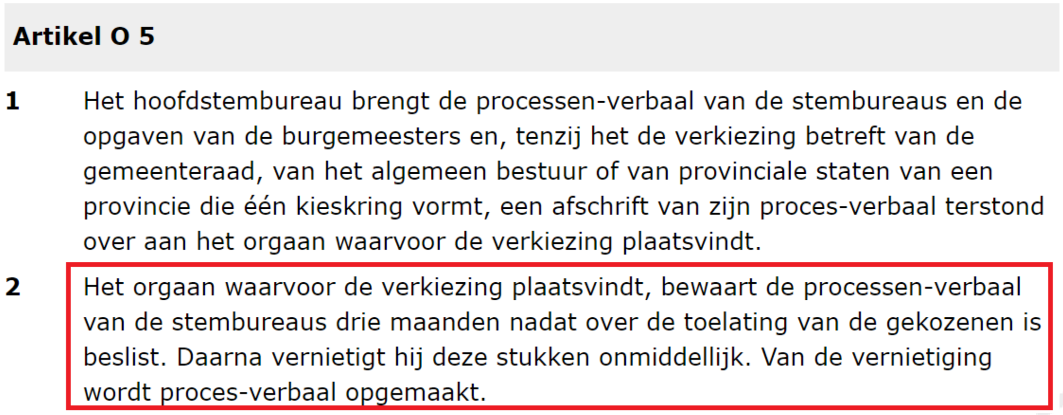
1 De burgemeester brengt de processen-verbaal en de opgave van de door hem vastgestelde aantallen stemmen onverwijld over naar het hoofdstembureau. Tevens legt hij een afschrift van deze stukken onverwijld voor een ieder ter inzage op het gemeentehuis totdat over de toelating van de gekozenen is beslist.

2 De burgemeester brengt de pakken, bedoeld in artikel N 9, op verzoek van het centraal stembureau over naar het centraal stembureau.

3 De burgemeester bewaart de pakken, bedoeld in de artikelen N 2 en N 9, die niet naar het centraal stembureau zijn overgebracht, en de afschriften, bedoeld in het eerste lid, drie maanden nadat over de toelating van de gekozenen is beslist. Daarna vernietigt hij deze stukken onmiddellijk, tenzij:

- **a.** de officier van justitie of de rechter-commissaris in het kader van een strafrechtelijk onderzoek een verzoek heeft gedaan tot overdracht van deze stukken, in welk geval de vernietiging plaatsvindt nadat dit onderzoek is afgerond;
- **b.** strafvervolging is ingesteld wegens een strafbaar gestelde gedraging in de Kieswet, de artikelen 125 tot en met 129 van het Wetboek van Strafrecht of de artikelen 131 tot en met 135 van het Wetboek van Strafrecht BES, in welk geval de vernietiging plaatsvindt nadat er een onherroepelijke rechterlijke uitspraak is.

4 Van de vernietiging wordt proces-verbaal opgemaakt.



Artikel O 5

1 Het hoofdstembureau brengt de processen-verbaal van de stembureaus en de opgaven van de burgemeesters en, tenzij het de verkiezing betreft van de gemeenteraad, van het algemeen bestuur of van provinciale staten van een provincie die één kieskring vormt, een afschrift van zijn proces-verbaal terstond over aan het orgaan waarvoor de verkiezing plaatsvindt.

2 Het orgaan waarvoor de verkiezing plaatsvindt, bewaart de processen-verbaal van de stembureaus drie maanden nadat over de toelating van de gekozenen is beslist. Daarna vernietigt hij deze stukken onmiddellijk. Van de vernietiging wordt proces-verbaal opgemaakt.

[18] See Election Law (Kieswet) article N 12 point 3 and article O 5 point 2: http://wetten.overheid.nl/jci1.3:c:BWBR0004627&afdeling=II&hoofdstuk=N&paragraaf=1&artikel=N_12&z=2017-12-01&g=2017-12-01

[19] See: http://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/

3 Retesting existing found vulnerabilities

On January 30, 2017 Sijmen Ruwhof published on his weblog a detailed technical analysis of all the weaknesses he found in OSV P4 and P5[20]. A retest has been performed to see if the findings mentioned on his weblog were resolved in the latest version of OSV. The following table lists each finding and the retest result:

ID	Vulnerability found in 2017	Situation is 2018: Reflection on current situation	See chapter	Retest result	Risk rating
1	Optional final paper audit.	After RTL News went live with the research about OSV insecurity, OSV output was not trusted anymore in the 2017 election. The totalization process was manually performed by the municipalities. After the elections, the Electoral Council has processed the security recommendations made by Fox IT and released a new OSV version for the upcoming elections. OSV is claimed to be secure again by the Electoral Council and thus the manual totalization effort is not required anymore by municipalities. The paper totalization process is not mandatory again.	4.1.1	Reopend	Critical
4	The voting software-application can be installed on any computer.	The Electoral Council published new security recommendations in 2017 that municipalities should enforce. If this policy is implemented correctly is not checked and enforced by OSV and not audited by the Electoral Council.	4.1.11, 4.1.12, 4.4.1	Unsolved	High
7	Voting software allows skipping SHA1 check.	OSV allows in some cases to skip the SHA256 validation by not enforcing the user the enter the full SHA256 code.	4.1.19	Unsolved	High
22	No automatic SHA1 hash check is in place for XML files stored on the computer.	Nothing has changed since last year and no automated OSV integrity checks are in place.	4.1.2, 4.1.18	Unsolved	High
33	The integrity of the software is hard to validate, and even optional.	1. The integrity of OSV installation files is now much more easier to validate, but still optional for system administrators at municipalities. 2. The integrity of OSV is only checked once, when installing it. The integrity of the OSV server is not validated again when the election is over. 3. The German company behind OSV could be compromised by a nation state and a	4.5.1, 4.1.10, 4.5.1	Partially solved	High

[20] See: https://sijmen.ruwhof.net/weblog/1166-how-to-hack-the-upcoming-dutch-elections

		hard to find backdoor could be included in OSV.		🟨	🟥
9	The voting software stores voting results in an unencrypted XML file.	This is still the case. But as the XML file is not transferred via USB stick anymore, it only resides on the OSV server itself. Still easy to tamper with if an adversary as gained access to the OSV server. Risk rating downgraded to medium.	**4.1.18**	**Unsolved**	**~~High~~** **Medium**
23	Voting results are sent via an unencrypted e-mail over the internet.	Nothing has changed in and this is still on-going practice. The voting results are only send by mail for archive purposes. Risk rating downgraded to medium.	**4.1.17**	**Unsolved**	**~~High~~** **Medium**
3	The voting-software initial installs a web server on the user's computer. Users have to open a web browser before they can use the voting-software.		**4.1.11,** **4.1.12**	**Unsolved**	**Medium**
18	No password strength policy is in place.	OSV now shows how strong a given password is, but allows one letter passwords to be set. Fox IT has also reported this vulnerability.	**4.1.22**	**Unsolved**	**Medium**
19	The Java session identifier is visible in the internet address.	Nothing has changed. Fox IT has also reported this vulnerability.	**4.1.5**	**Unsolved**	**Medium**
20	Instructor uses Windows administrator account instead of low privileged account. The software allows this.	Still recommended practice by OSV documentation.		**Unsolved**	**Medium**
21	Software saves high integrity XML files into a public location on the computer.			**Unsolved**	**Medium**
27	It is partly open source.	The OSV P4 and P5 software is semi public. It is not downloadable on www.kiesraad.nl and a CD-ROM should be manually requested. There is no transparency on what exact operating system and network infrastructure is used to host OSV on in hopefully air-gapped networks at municipalities.	**4.1.11,** **4.1.12,** **4.4.1**	**Unsolved**	**Medium**
28	A cross-site scripting vulnerability was found.	Nothing has changed. More cross-site scripting vulnerabilities have been found.	**4.1.20**	**Unsolved**	**Medium**
30	No intrusion detection systems are active.	Nothing has changed.	**4.1.9**	**Unsolved**	**Medium**
24	Most sensitive operations in voting software have least SHA1 protection	When uploading an EML file that contains voting totals, then OSV makes the user enter eight characters of the SHA256 code, not the full SHA256 code.		**Partially solved**	**~~High~~** **Medium**
25	Internet connected computers.	Municipalities are now much better instructed that internet access is not allowed. The OSV server keeps running even is an internet	**4.1.15**	**Partially solved**	**~~High~~** **Medium**

		connection is present however. OSV does not enforce this security policy.			
5	The browser for the election software connects to a local host via an unsecured HTTP connection.		**4.1.23**	**Partially solved**	**Medium**
12	The architect designed the system, but it seems that this person does not review the generated (security) documentation about it.	OSV is now accompanied with security documentation. This documentation is however limited.		**Partially solved**	**Medium**
14	Custom USB sticks can be used, and these sticks can be loaded with malicious software.	Election results won't be transferred by USB sticks anymore to the Electoral Council for election determination. The Electoral Council receives however USB sticks from political parties to receive candidate lists.	**4.4.2**	**Partially solved**	**Medium**
26	No IT security expert was consulted when building this software.	Fox-IT was hired in January 2017 by the Electoral Council, but was not hired again to retest the new OSV version.		**Partially solved**	**Medium**
29	Logs are not collected on a central server and thus easy to tamper with.	Logs are not collected on a central server and thus easy to tamper with. System administrators are instructed to download all EML and log files and burn them onto a CD-ROM and store it locally for 90 days.	**2.1.2**	**Partially solved**	**Medium**
31	No experienced ethical hacker has reviewed the software.	Fox-IT was hired in January 2017 by the Electoral Council, but wasn't hired again to retest the new OSV version.		**Partially solved**	**Medium**
15	Web browser automatically completes user passwords on a shared computer.	In the newest OSV version the login form has the `autocomplete=off` setting set and thus this finding can be closed. It should be noted that modern browsers automatically complete passwords and ignore the `autocomplete=off` setting. If a OSV client computer is used by multiple people under the same operating system user account, then this risk is still there.		**Solved**	**Medium**
17	A non-personal user account is used.	The OSV administrator account is still named `osv`.	**4.1.30**	**Unsolved**	**Low**
2	Eight internal network shares (from an internal server called Amsterdam) are visible in a YouTube video.	The YouTube video found in 2017 has been removed by the Electoral Council. A new YouTube video has been found in which internal network shares from IVU are shown.	**4.5.3**	**Reopend**	**Very low**

6	Instructor skips important SHA1 check in YouTube video.	The YouTube video has been removed by the Electoral Council.		Solved	High
8	The insecure, old and deprecated SHA1 hash algorithm is used everywhere in the software.	The SHA1 hash algorithm has been changed by SHA256.		Solved	High
10	PDF file with SHA1 hash code is stored next to corresponding XML file it has to protect.	Election results won't be transferred by USB sticks anymore to the Electoral Council for election determination.		Solved	Medium
11	The voting software / instructor does not mention that PDF files should be printed, nor enforces you to manually delete generated PDF files.	Election results won't be transferred by USB sticks anymore to the Electoral Council for election determination.		Solved	Medium
13	Non-encrypted USB sticks are used.	Election results won't be transferred by USB sticks anymore to the Electoral Council for election determination.		Solved	High
16	Instructor uses three letter password.	The YouTube video has been removed by the Electoral Council.		Solved	Medium
32	No security test reports are available.	Fox-IT was hired in January 2017 by the Electoral Council, but wasn't hired again to retest the new OSV version. The complete Fox IT report from 2017 was published by the Electoral Council on their website.		Solved	Medium

Statistics about solved findings:

Status	Total findings
Total vulnerabilities unsolved	16
Total vulnerabilities partly solved	9
Total vulnerabilities solved	8

There are 25 open security risks after the retest (all unsolved and partly solved findings):

Total findings	Risk
1	Critical
4	High
18	Medium
1	Low
1	Very low

4 List of identified security risks

This this chapter all existing and newly identified security risks in OSV P4 and P5 are documented.

4.1 In OSV server and clients

4.1.1 Critial: OSV prints paper that will become leading

RTL News found out that the Electoral Council and municipalities silently trusted OSV output again and will use it to calculate who will win the upcoming elections on March 21, 2018. This renewed trust in OSV was also not validated by an independent respectable cyber security firm. The Electoral Council did not hire Fox IT again in 2018 to check if all major security risks were properly solved in the new OSV version made by IVU.

After election day on March 22, 2018, civil servants from the central vote office of a municipality will enter vote totals from polling stations into OSV (see chapter 4.1.1). OSV will totalize all vote totals per candidate and generate a PDF file that contains the election result that has to be printed (a so-called N11 and O3 document). The printed election result becomes official and trusted 'paper that is in the lead'. It will not be manually validated by civil servants as OSV is trusted to be unhackable again.

Impact
If someone hacks the OSV server, then this person can manipulate votes by changing votes stored in the OSV database and in the PDF files stored on the server that have to be printed.

Recommendation
Do not trust output from OSV again. Use OSV to only validate votes counted manually. History shows that exclusive manual aggregation of vote totals is error-prone[21], and exclusive digital aggregation of vote totals is vulnerable to manipulation by sophisticated attackers[22].

OSV can be useful however, even to strengthen the security of an election. All vote totals for each candidate from a political party should be manually totalized by the central vote office of a municipality. Afterwards, the vote totals as calculated by each independent polling station in a municipality should be entered into OSV. OSV should also totalize all vote totals and calculate who won the election. OSV output should be used to verify if the manual totalization is done properly and without mistakes.

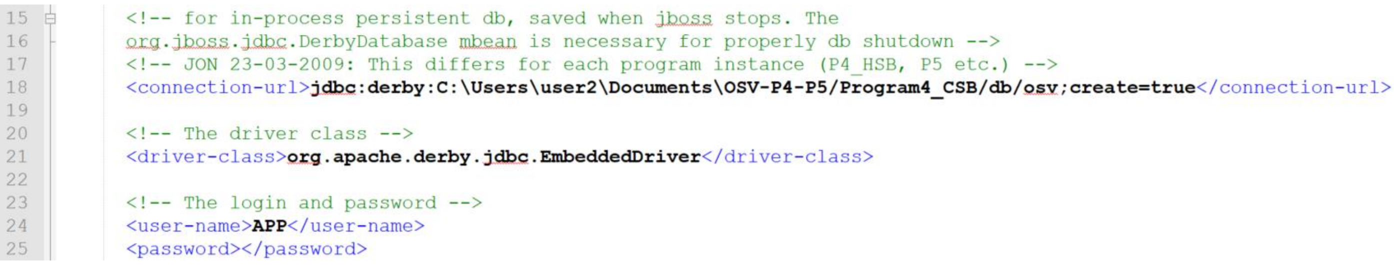
Untrusting OSV and manually totalizing vote totals takes a couple more days to perform, but eliminates all the risks that our election can be hacked by manipulating vote totals. Waiting a couple more days on the election outcome is nothing compared to the impact if the election gets hacked. Official paper vote total reports of municipalities should be manually be filled in by civil servants based on the manual calculated vote totals. OSV prints should never be used as official documents anymore. The cyber security of OSV is of much less importance if its output is distrusted.

[21] See news story from June 13, 2017: https://www.trouw.nl/home/veel-stemmen-verkeerd-geteld-bij-kamerverkiezingen~ab6e2a02/
See news story from March 28, 2017: https://www.rtlnieuws.nl/nederland/politiek/van-alles-misgegaan-bij-optellen-stemmen-verkiezingen

[22] As proven by RTL News and Sijmen Ruwhof on January 30, 2017 and by Fox IT in their report published on March 3, 2017.

4.1.2 High: OSV database can be easily modified and votes can be changed

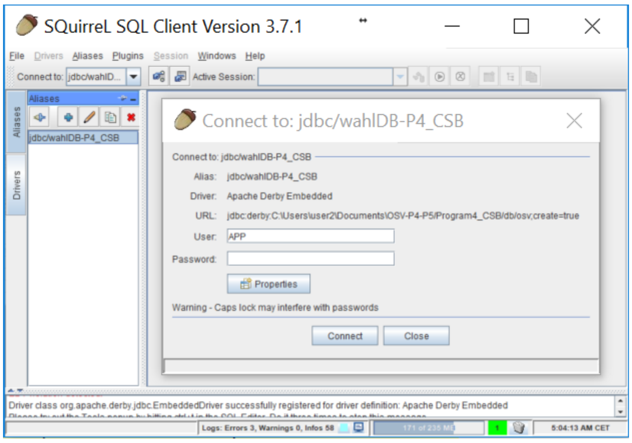
The file `\jboss-4.2.3.GA\server\osv\deploy\derby-ds.xml` on the OSV server contains the database login credentials of the Derby database server that is used by OSV P4 and P5:



```
<!-- for in-process persistent db, saved when jboss stops. The
org.jboss.jdbc.DerbyDatabase mbean is necessary for properly db shutdown -->
<!-- JON 23-03-2009: This differs for each program instance (P4_HSB, P5 etc.) -->
<connection-url>jdbc:derby:C:\Users\user2\Documents\OSV-P4-P5/Program4_CSB/db/osv;create=true</connection-url>

<!-- The driver class -->
<driver-class>org.apache.derby.jdbc.EmbeddedDriver</driver-class>

<!-- The login and password -->
<user-name>APP</user-name>
<password></password>
```

Opening the Derby database

By installing SQuirrel SQL Client on the OSV server it was possible to connect to the Derby database OSV uses:



Connect to: jdbc/wahlDB-P4_CSB

Alias: jdbc/wahlDB-P4_CSB

Driver: Apache Derby Embedded

URL: jdbc:derby:C:\Users\user2\Documents\OSV-P4-P5/Program4_CSB/db/osv;create=true

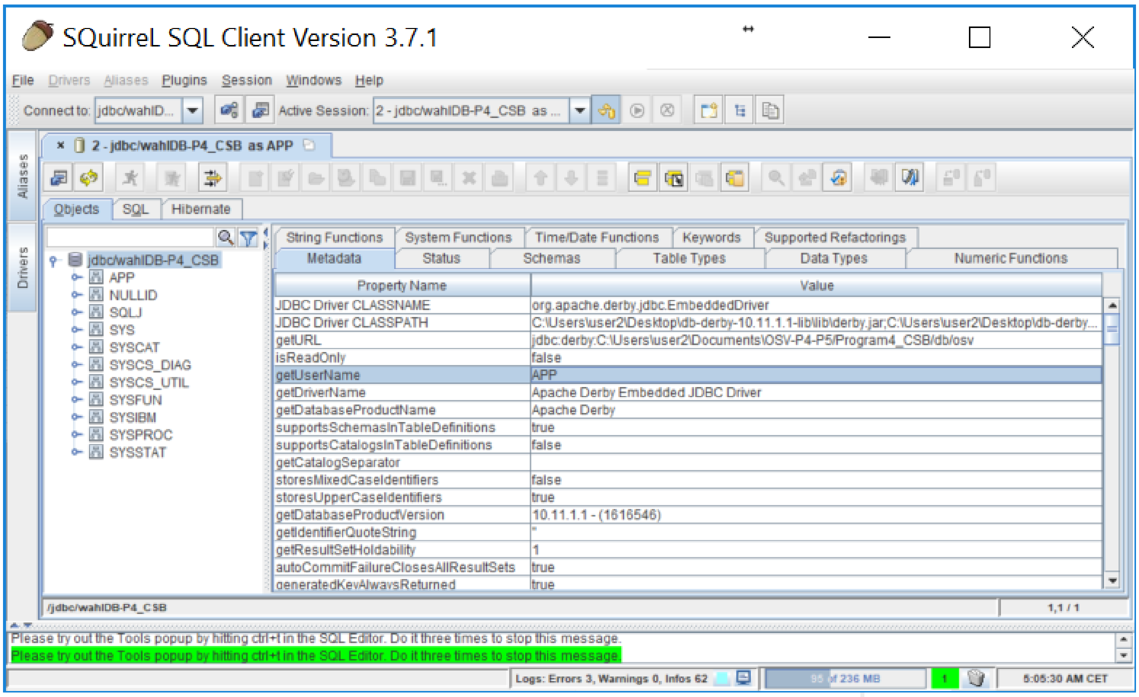
User: APP

Password:

Warning - Caps lock may interfere with passwords

Driver class org.apache.derby.jdbc.EmbeddedDriver successfully registered for driver definition: Apache Derby Embedded

With user `APP` and with no password (see also chapter 4.1.16) given it was possible to open the OSV database:



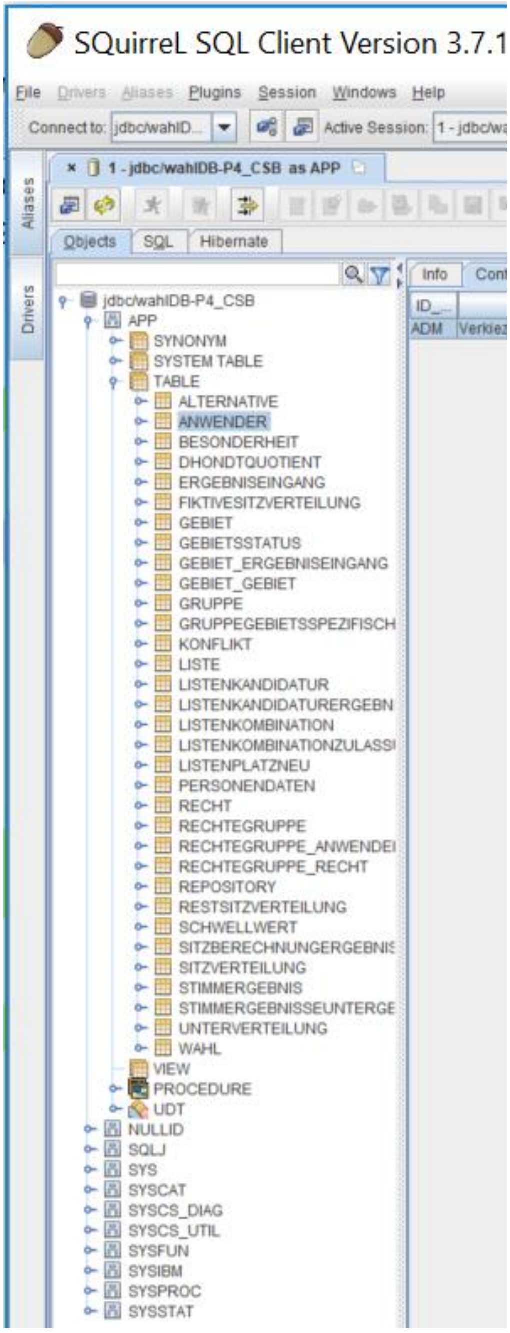
Property Name	Value
JDBC Driver CLASSNAME	org.apache.derby.jdbc.EmbeddedDriver
JDBC Driver CLASSPATH	C:\Users\user2\Desktop\db-derby-10.11.1.1-lib\lib\derby.jar;C:\Users\user2\Desktop\db-derby...
getURL	jdbc:derby:C:\Users\user2\Documents\OSV-P4-P5/Program4_CSB/db/osv
isReadOnly	false
getUserName	APP
getDriverName	Apache Derby Embedded JDBC Driver
getDatabaseProductName	Apache Derby
supportsSchemasInTableDefinitions	true
supportsCatalogsInTableDefinitions	false
getCatalogSeparator	
storesMixedCaseIdentifiers	false
storesUpperCaseIdentifiers	true
getDatabaseProductVersion	10.11.1.1 - (1616546)
getIdentifierQuoteString	"
getResultSetHoldability	1
autoCommitFailureClosesAllResultSets	true
generatedKeyAlwaysReturned	true

Please try out the Tools popup by hitting ctrl+t in the SQL Editor. Do it three times to stop this message.

Please try out the Tools popup by hitting ctrl+t in the SQL Editor. Do it three times to stop this message.

OSV database tables

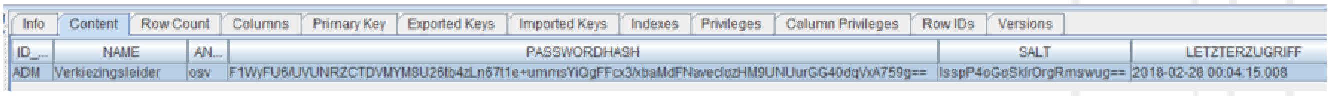
OSV uses the `APP` database. This database has the following tables:


SQuirreL SQL Client Version 3.7.1
File Drivers Aliases Plugins Session Windows Help
Connect to: jdbc/wahlD...
Active Session: 1 - jdbc/wa
1 - jdbc/wahlDB-P4_CSB as APP
Aliases
Drivers
Objects SQL Hibernate
Info Cont
ID_...
ADM Verkiez

```
jdbc/wahlDB-P4_CSB
  APP
    SYNONYM
    SYSTEM TABLE
    TABLE
      ALTERNATIVE
      ANWENDER
      BESONDERHEIT
      DHONDTQUOTIENT
      ERGEBNISEINGANG
      FIKTIVESITZVERTEILUNG
      GEBIET
      GEBIETSSTATUS
      GEBIET_ERGEBNISEINGANG
      GEBIET_GEBIET
      GRUPPE
      GRUPPEGEBIETSSPEZIFISCH
      KONFLIKT
      LISTE
      LISTENKANDIDATUR
      LISTENKANDIDATURERGEBN
      LISTENKOMBINATION
      LISTENKOMBINATIONZULASSI
      LISTENPLATZNEU
      PERSONENDATEN
      RECHT
      RECHTEGRUPPE
      RECHTEGRUPPE_ANWENDEI
      RECHTEGRUPPE_RECHT
      REPOSITORY
      RESTSITZVERTEILUNG
      SCHWELLWERT
      SITZBERECHNUNGERGEBNIS
      SITZVERTEILUNG
      STIMMERGEBNIS
      STIMMERGEBNISSEUNTERGE
      UNTERVERTEILUNG
      WAHL
    VIEW
    PROCEDURE
    UDT
  NULLID
  SQLJ
  SYS
  SYSCAT
  SYSCS_DIAG
  SYSCS_UTIL
  SYSFUN
  SYSIBM
  SYSPROC
  SYSSTAT
```

Passwords are securely stored

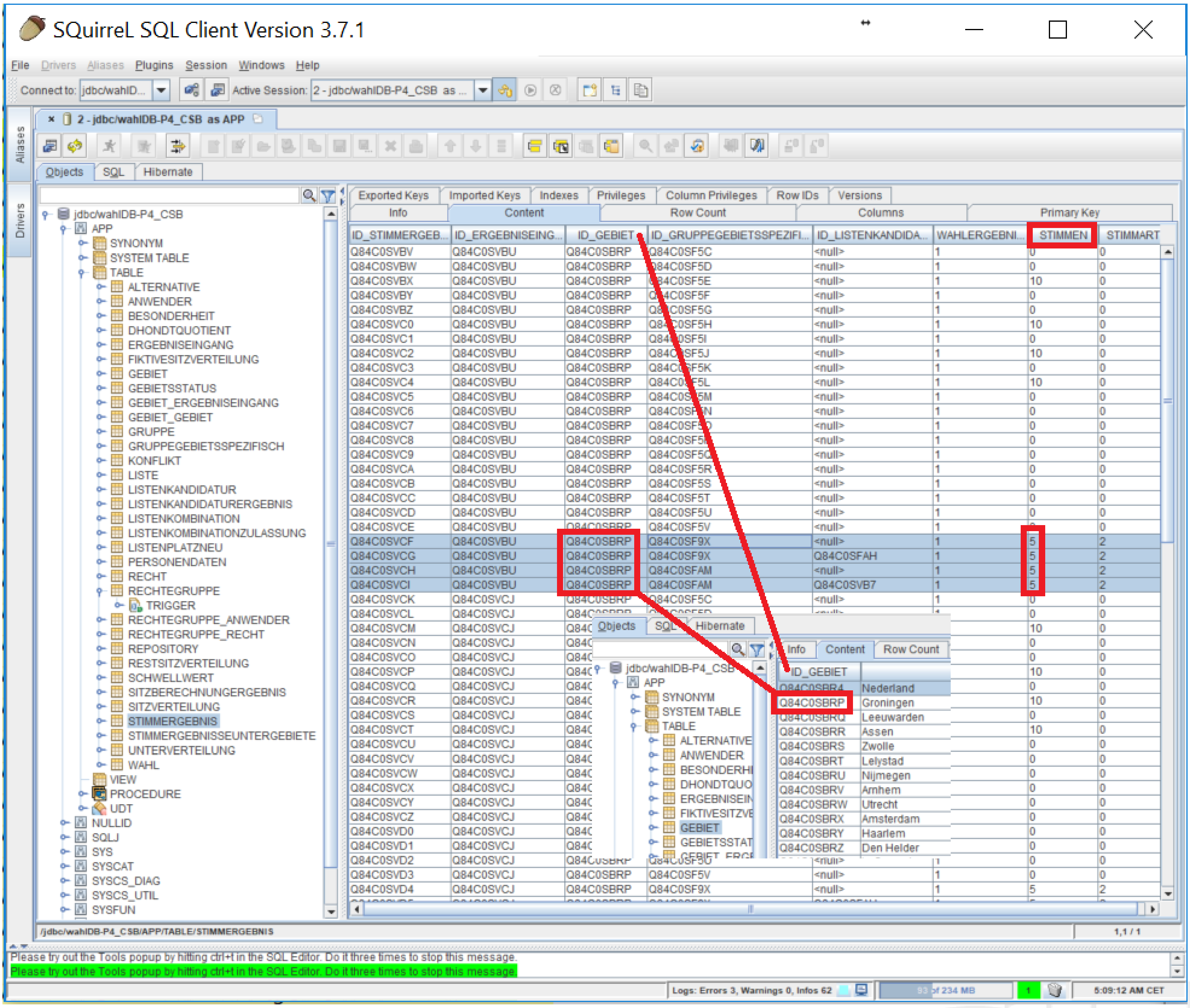
Fox IT made a finding that passwords were insecure stored by OSV. This finding seems to be soled as passwords are now properly salted before storing them into database table `ANWENDER`.



ID_...	NAME	AN...	PASSWORDHASH	SALT	LETZTERZUGRIFF
ADM	Verkiezingsleider	osv	F1WyFU6/UVUNRZCTDVMYM8U26tb4zLn67t1e+ummsYiQgFFcx3/xbaMdFNaveclozHM9UNUurGG40dqVxA759g==	IsspP4oGoSklrOrgRmswug==	2018-02-28 00:04:15.008

Manipulating votes

When OSV users have entered vote totals into OSV P4, these totals are then stored in the `STIMMEN` column in the `STIMMERGEBNIS` table. To test if votes could be manipulated in the database, the referendum definition was loaded in P4 that will be used by the Electoral Council. For Groningen the total votes entered into OSV against the new law were 8, and 2 people would agree with the law in the test scenario. After entering the vote totals in the OSV interface, the vote totals could be easily found in the `STIMMERGEBNIS` table. The 8 votes were changed via SQuirrel SQL Client to 5 votes against the law, and 5 votes that agree with the law to see if OSV would notice this manipulation:

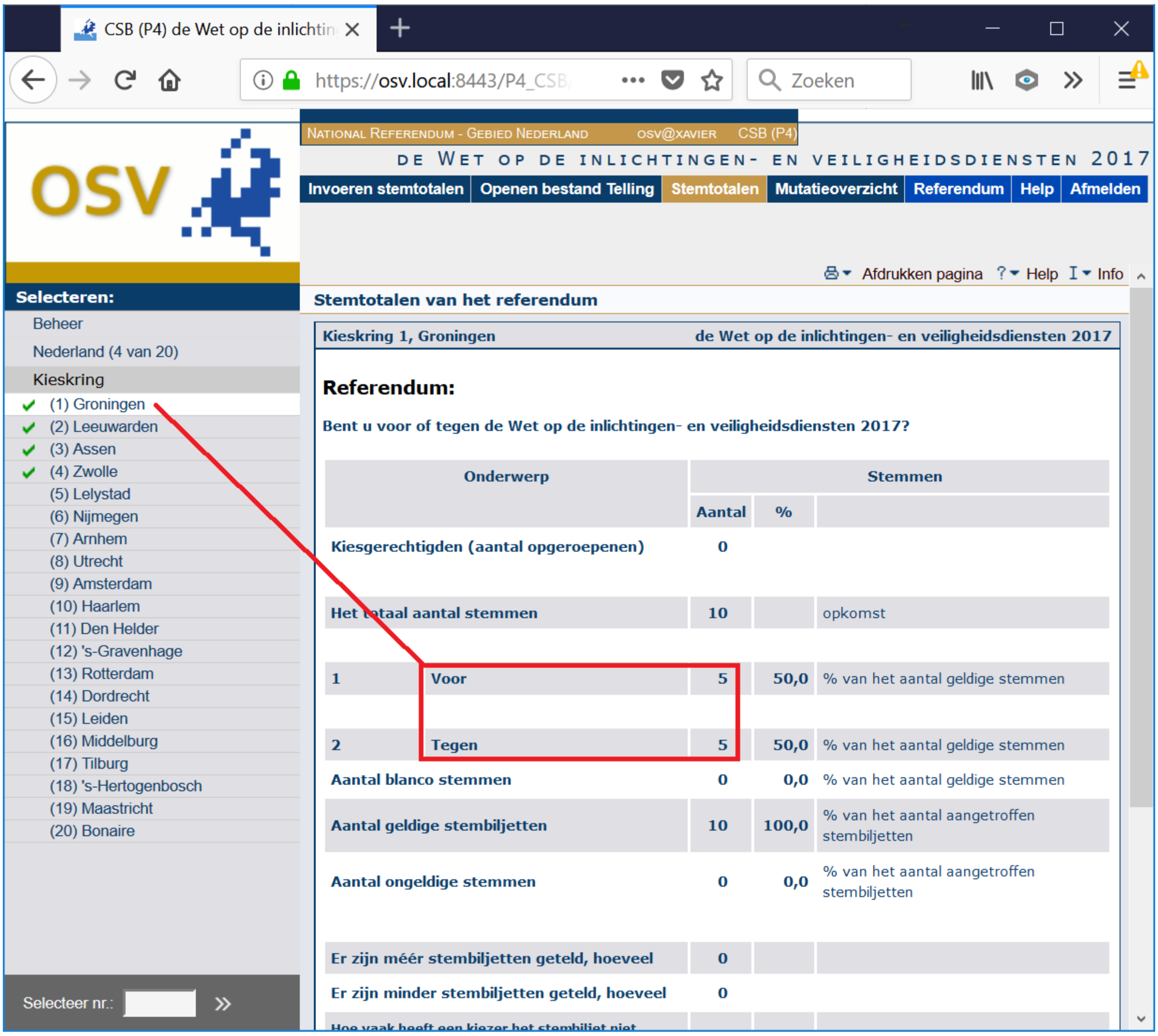


ID_STIMMERGEB...	ID_ERGEBNISEING...	ID_GEBIET	ID_GRUPPEGEBIETSSPEZIFI...	ID_LISTENKANDIDA...	WAHLERGEBNI...	STIMMEN	STIMMART
Q84C0SVBV	Q84C0SVBU	Q84C0SBRP	Q84C0SF5C	<null>	1	0	0
Q84C0SVBW	Q84C0SVBU	Q84C0SBRP	Q84C0SF5D	<null>	1	0	0
Q84C0SVBX	Q84C0SVBU	Q84C0SBRP	Q84C0SF5E	<null>	1	10	0
Q84C0SVBY	Q84C0SVBU	Q84C0SBRP	Q84C0SF5F	<null>	1	0	0
Q84C0SVBZ	Q84C0SVBU	Q84C0SBRP	Q84C0SF5G	<null>	1	0	0
Q84C0SVC0	Q84C0SVBU	Q84C0SBRP	Q84C0SF5H	<null>	1	10	0
Q84C0SVC1	Q84C0SVBU	Q84C0SBRP	Q84C0SF5I	<null>	1	0	0
Q84C0SVC2	Q84C0SVBU	Q84C0SBRP	Q84C0SF5J	<null>	1	10	0
Q84C0SVC3	Q84C0SVBU	Q84C0SBRP	Q84C0SF5K	<null>	1	0	0
Q84C0SVC4	Q84C0SVBU	Q84C0SBRP	Q84C0SF5L	<null>	1	10	0
Q84C0SVC5	Q84C0SVBU	Q84C0SBRP	Q84C0SF5M	<null>	1	0	0
Q84C0SVC6	Q84C0SVBU	Q84C0SBRP	Q84C0SF5N	<null>	1	0	0
Q84C0SVC7	Q84C0SVBU	Q84C0SBRP	Q84C0SF5O	<null>	1	0	0
Q84C0SVC8	Q84C0SVBU	Q84C0SBRP	Q84C0SF5P	<null>	1	0	0
Q84C0SVC9	Q84C0SVBU	Q84C0SBRP	Q84C0SF5Q	<null>	1	0	0
Q84C0SVCA	Q84C0SVBU	Q84C0SBRP	Q84C0SF5R	<null>	1	0	0
Q84C0SVCB	Q84C0SVBU	Q84C0SBRP	Q84C0SF5S	<null>	1	0	0
Q84C0SVCC	Q84C0SVBU	Q84C0SBRP	Q84C0SF5T	<null>	1	0	0
Q84C0SVCD	Q84C0SVBU	Q84C0SBRP	Q84C0SF5U	<null>	1	0	0
Q84C0SVCE	Q84C0SVBU	Q84C0SBRP	Q84C0SF5V	<null>	1	0	0
Q84C0SVCF	Q84C0SVBU	Q84C0SBRP	Q84C0SF9X	<null>	1	5	2
Q84C0SVCG	Q84C0SVBU	Q84C0SBRP	Q84C0SF9X	Q84C0SFAH	1	5	2
Q84C0SVCH	Q84C0SVBU	Q84C0SBRP	Q84C0SFAM	<null>	1	5	2
Q84C0SVCI	Q84C0SVBU	Q84C0SBRP	Q84C0SFAM	Q84C0SVB7	1	5	2
Q84C0SVCK	Q84C0SVCJ	Q84C0SBRP	Q84C0SF5C	<null>	1	0	0
Q84C0SVCL	Q84C0SVCJ	Q84C0SBRP	Q84C0SF5D	<null>	1	0	0
Q84C0SVCM	Q84C0SVCJ	Q84C				10	0
Q84C0SVCN	Q84C0SVCJ	Q84C				0	0
Q84C0SVCO	Q84C0SVCJ	Q84C				0	0
Q84C0SVCP	Q84C0SVCJ	Q84C				10	0
Q84C0SVCQ	Q84C0SVCJ	Q84C				0	0
Q84C0SVCR	Q84C0SVCJ	Q84C				10	0
Q84C0SVCS	Q84C0SVCJ	Q84C				0	0
Q84C0SVCT	Q84C0SVCJ	Q84C				10	0
Q84C0SVCU	Q84C0SVCJ	Q84C				0	0
Q84C0SVCV	Q84C0SVCJ	Q84C				0	0
Q84C0SVCW	Q84C0SVCJ	Q84C				0	0
Q84C0SVCX	Q84C0SVCJ	Q84C				0	0
Q84C0SVCY	Q84C0SVCJ	Q84C				0	0
Q84C0SVCZ	Q84C0SVCJ	Q84C				0	0
Q84C0SVD0	Q84C0SVCJ	Q84C				0	0
Q84C0SVD1	Q84C0SVCJ	Q84C				0	0
Q84C0SVD2	Q84C0SVCJ	Q84C0SBRP	Q84C0SF5U	<null>	1	0	0
Q84C0SVD3	Q84C0SVCJ	Q84C0SBRP	Q84C0SF5V	<null>	1	0	0
Q84C0SVD4	Q84C0SVCJ	Q84C0SBRP	Q84C0SF9X	<null>	1	5	2

ID_GEBIET	
Q84C0SBR4	Nederland
Q84C0SBRP	Groningen
Q84C0SBRQ	Leeuwarden
Q84C0SBRR	Assen
Q84C0SBRS	Zwolle
Q84C0SBRT	Lelystad
Q84C0SBRU	Nijmegen
Q84C0SBRV	Arnhem
Q84C0SBRW	Utrecht
Q84C0SBRX	Amsterdam
Q84C0SBRY	Haarlem
Q84C0SBRZ	Den Helder

```
Please try out the Tools popup by hitting ctrl+t in the SQL Editor. Do it three times to stop this message.
Please try out the Tools popup by hitting ctrl+t in the SQL Editor. Do it three times to stop this message.
```

After the vote manipulation was executed, the OSV server was started again. OSV shows the manipulated vote total as if nothing had happened:



Selecteren:
Beheer
Nederland (4 van 20)
Kieskring
✓ (1) Groningen
✓ (2) Leeuwarden
✓ (3) Assen
✓ (4) Zwolle
(5) Lelystad
(6) Nijmegen
(7) Arnhem
(8) Utrecht
(9) Amsterdam
(10) Haarlem
(11) Den Helder
(12) 's-Gravenhage
(13) Rotterdam
(14) Dordrecht
(15) Leiden
(16) Middelburg
(17) Tilburg
(18) 's-Hertogenbosch
(19) Maastricht
(20) Bonaire

Stemtotalen van het referendum

Kieskring 1, Groningen — **de Wet op de inlichtingen- en veiligheidsdiensten 2017**

Referendum:

Bent u voor of tegen de Wet op de inlichtingen- en veiligheidsdiensten 2017?

Onderwerp		Stemmen		
		Aantal	%	
Kiesgerechtigden (aantal opgeroepenen)		0		
Het totaal aantal stemmen		10		opkomst
1	Voor	5	50,0	% van het aantal geldige stemmen
2	Tegen	5	50,0	% van het aantal geldige stemmen
Aantal blanco stemmen		0	0,0	% van het aantal geldige stemmen
Aantal geldige stembiljetten		10	100,0	% van het aantal aangetroffen stembiljetten
Aantal ongeldige stemmen		0	0,0	% van het aantal aangetroffen stembiljetten
Er zijn méér stembiljetten geteld, hoeveel		0		
Er zijn minder stembiljetten geteld, hoeveel		0		
Hoe vaak heeft een kiezer het stembiljet niet				

Impact

It is very easy to alter votes directly via the Derby database on the OSV server. A hacker could only perform this manipulation if it has gained access to the OSV server. OSV does not detect manipulation of votes.

When an adversary has gained access to the OSV server then it is very easy to alter votes in OSV:

1. By compromising the supply chain of OSV (see chapter 4.5.1 and 4.5.4).
2. By injecting implants into BYOD from municipalities that function as a stepping-stone and are deployed in the OSV network (see chapter 4.3.1),
3. This hack could also be easily done by a system administrator of a municipality or a foreign intelligence agency (see chapter 0).

The Fox IT report also mentions:

- *"[..] **3.1.2 Gemeentes (PSB en HSB)***
  Aan gemeentes (PSB's en HSB's) worden richtlijnen verstrekt om ten behoeve van OSV gebruik te maken van systemen die geen koppeling met het internet hebben. Voor kleinere gemeentes betekent dit dat veelal gebruik zal worden gemaakt van een "stand alone" computer met daarop OSV. Voor grotere gemeentes geldt dat dan gebruik wordt gemaakt van een "afgeschermd" netwerk met daarin een systeem dat als OSV (web)server dient en meerdere systemen die als client dienen. Deze clients benaderen de OSV- webapplicatie dan vanuit de browser.

  De webapplicatie wordt volgens de richtlijnen in verschillende omgevingen gebruikt, waaronder:

  1. *"Stand-alone" systeem (zonder netwerkverbindingen)*
  2. *Centrale server met meerdere clients ("afgeschermd" netwerk)*

  Wanneer de webapplicatie op een "stand alone" systeem zonder netwerkverbinding wordt gebruikt, dan bevindt het servercomponent en het clientcomponent zich op een en hetzelfde systeem. [..]"

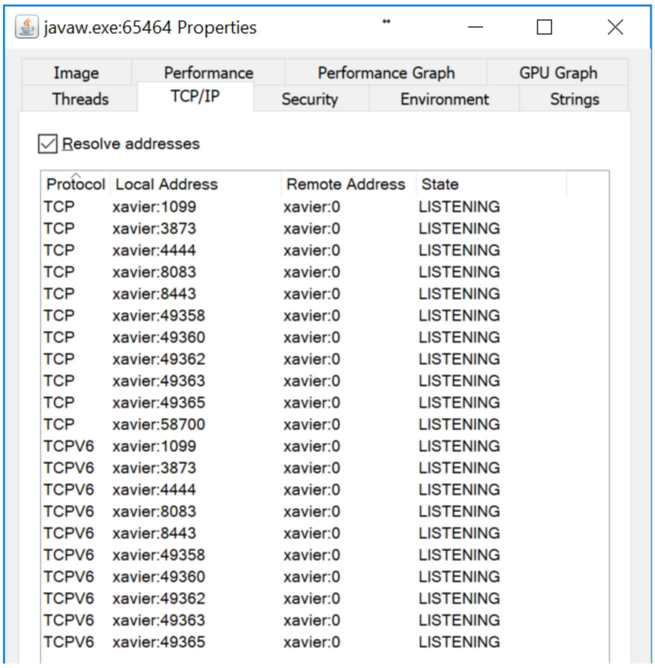
In small municipalities OSV will be used on a stand-alone computer with no network connection. This means that multiple OSV users will work on the same computer, and probably also under the same operating system user account. When OSV is used on a stand-alone computer and when installed improperly, all OSV users on that computer could access the Derby database and manipulate with the votes if the database. The OSV security documentation does not advice on how to protect the OSV database if OSV is used on a stand-alone computer.

4.1.3 High: Unnecessary ports are opened by Java

Risk :	High
Location :	osv.local TCP port 1099, 3873, 4444 and 8083
Description :	When the OSV server is started, OSV is opening port `1099`, `3873`, `4444`, `8083` and `8443` on the server via `java.exe`. Only port `8443` which offers the HTTPS interface for OSV clients should be exposed on the server.
Impact :	Only port `8443` should be opened on the server. Unnecessary ports widens the attack surface of an attacker, thereby making the host more vulnerable to attacks. As the JBoss and Java SE server software is not patched for many years, it is a very bad idea exposing these vulnerable services towards the internal network. Other computers connected to the internal network can probably hack the OSV server via the 4 unnecessary exposed services.
Recommendation :	Make sure that the open ports that are unnecessary for the functioning of the server be shut down.

Reproduction :	Run Nmap from another computer connected to the internal network and perform a port scan on the OSV server:
	`nmap -sT -sV -p 1099,3648,3873,4444,8080,8083,8443 -O osv.local`
	`PORT      STATE SERVICE     REASON  VERSION`
	`1099/tcp  open  java-rmi    syn-ack Java RMI`
	`3873/tcp  open  java-rmi    syn-ack Java RMI`
	`4444/tcp  open  rmiregistry syn-ack Java RMI`
	`8083/tcp  open  us-srv?     syn-ack`
	`8443/tcp  open  ssl/http    syn-ack Apache Tomcat/Coyote JSP engine 1.1`

Evidence :



☑ Resolve addresses

```
Protocol Local Address   Remote Address  State
TCP      xavier:1099     xavier:0        LISTENING
TCP      xavier:3873     xavier:0        LISTENING
TCP      xavier:4444     xavier:0        LISTENING
TCP      xavier:8083     xavier:0        LISTENING
TCP      xavier:8443     xavier:0        LISTENING
TCP      xavier:49358    xavier:0        LISTENING
TCP      xavier:49360    xavier:0        LISTENING
TCP      xavier:49362    xavier:0        LISTENING
TCP      xavier:49363    xavier:0        LISTENING
TCP      xavier:49365    xavier:0        LISTENING
TCP      xavier:58700    xavier:0        LISTENING
TCPV6    xavier:1099     xavier:0        LISTENING
TCPV6    xavier:3873     xavier:0        LISTENING
TCPV6    xavier:4444     xavier:0        LISTENING
TCPV6    xavier:8083     xavier:0        LISTENING
TCPV6    xavier:8443     xavier:0        LISTENING
TCPV6    xavier:49358    xavier:0        LISTENING
TCPV6    xavier:49360    xavier:0        LISTENING
TCPV6    xavier:49362    xavier:0        LISTENING
TCPV6    xavier:49363    xavier:0        LISTENING
TCPV6    xavier:49365    xavier:0        LISTENING
```

```
\jboss-4.2.3.GA\server\osv\conf\jboss-service.xml

<!-- A mini webserver used for dynamic and class and resource loading -->
<mbean code="org.jboss.web.WebService"
name="jboss:service=WebService">
<!-- The Bind address and Port -->
<attribute name="BindAddress">${jboss.bind.address}</attribute>
<attribute name="Port">8083</attribute>
<!-- The address to use for the host portion of the RMI codebase URL -->
<attribute name="Host">${java.rmi.server.hostname}</attribute>
<!-- Should non-EJB .class files be downloadable -->
<attribute name="DownloadServerClasses">true</attribute>
<!-- Should resources other than .class files be downloadable. Both
DownloadServerClasses and DownloadResources must be true for resources
to be downloadable. This is false by default because its generally a
bad idea as server configuration files that container security
information can be accessed.
-->
<attribute name="DownloadResources">false</attribute>

<!-- Use the default thread pool for dynamic class loading -->
<depends optional-attribute-name="ThreadPool"
proxy-type="attribute">jboss.system:service=ThreadPool</depends>
</mbean>
<mbean code="org.jboss.naming.NamingService"
name="jboss:service=Naming"
xmbean-dd="resource:xmdesc/NamingService-xmbean.xml">
<!-- The call by value mode. true if all lookups are unmarshalled using
the caller's TCL, false if in VM lookups return the value by reference.
-->
<attribute name="CallByValue">true</attribute>
<!-- The listening port for the bootstrap JNP service. Set this to -1
to run the NamingService without the JNP invoker listening port.
-->
<attribute name="Port">1099</attribute>
<!-- The bootstrap JNP server bind address. This also sets the default
RMI service bind address. Empty == all addresses
-->
```

```
<attribute name="BindAddress">${jboss.bind.address}</attribute>
<!-- The port of the RMI naming service, 0 == anonymous -->
<attribute name="RmiPort">0</attribute>
<!-- The RMI service bind address. Empty == all addresses
-->
<attribute name="RmiBindAddress">${jboss.bind.address}</attribute>
<!-- The thread pool service used to control the bootstrap lookups -->
<depends optional-attribute-name="LookupPool"
proxy-type="attribute">jboss.system:service=ThreadPool</depends>
<!-- An example of using the unifed invoker as the transport.
<depends optional-attribute-name="InvokerProxyFactory"
proxy-
type="attribute">jboss:service=proxyFactory,type=unified,target=Naming</depen
ds>
-->
<depends optional-attribute-name="Naming"
proxy-type="attribute">jboss:service=NamingBeanImpl</depends>
</mbean>
<!-- RMI/JRMP invoker -->
<mbean code="org.jboss.invocation.jrmp.server.JRMPInvoker"
name="jboss:service=invoker,type=jrmp">
<attribute name="RMIObjectPort">4444</attribute>
<attribute name="ServerAddress">${jboss.bind.address}</attribute>
<!--
<attribute name="RMIClientSocketFactory">custom</attribute>
<attribute name="RMIServerSocketFactory">custom</attribute>
<attribute name="RMIServerSocketAddr">custom</attribute>
<attribute name="SecurityDomain">ssl-domain-name</attribute>
-->
<depends>jboss:service=TransactionManager</depends>
</mbean>
<hr>
\server\osv\log\boot.log

Using RMI server codebase: http://osv.local:8083/
```

Patch status :	Open (not solved)

The Fox IT report about ports opened on the OSV server:

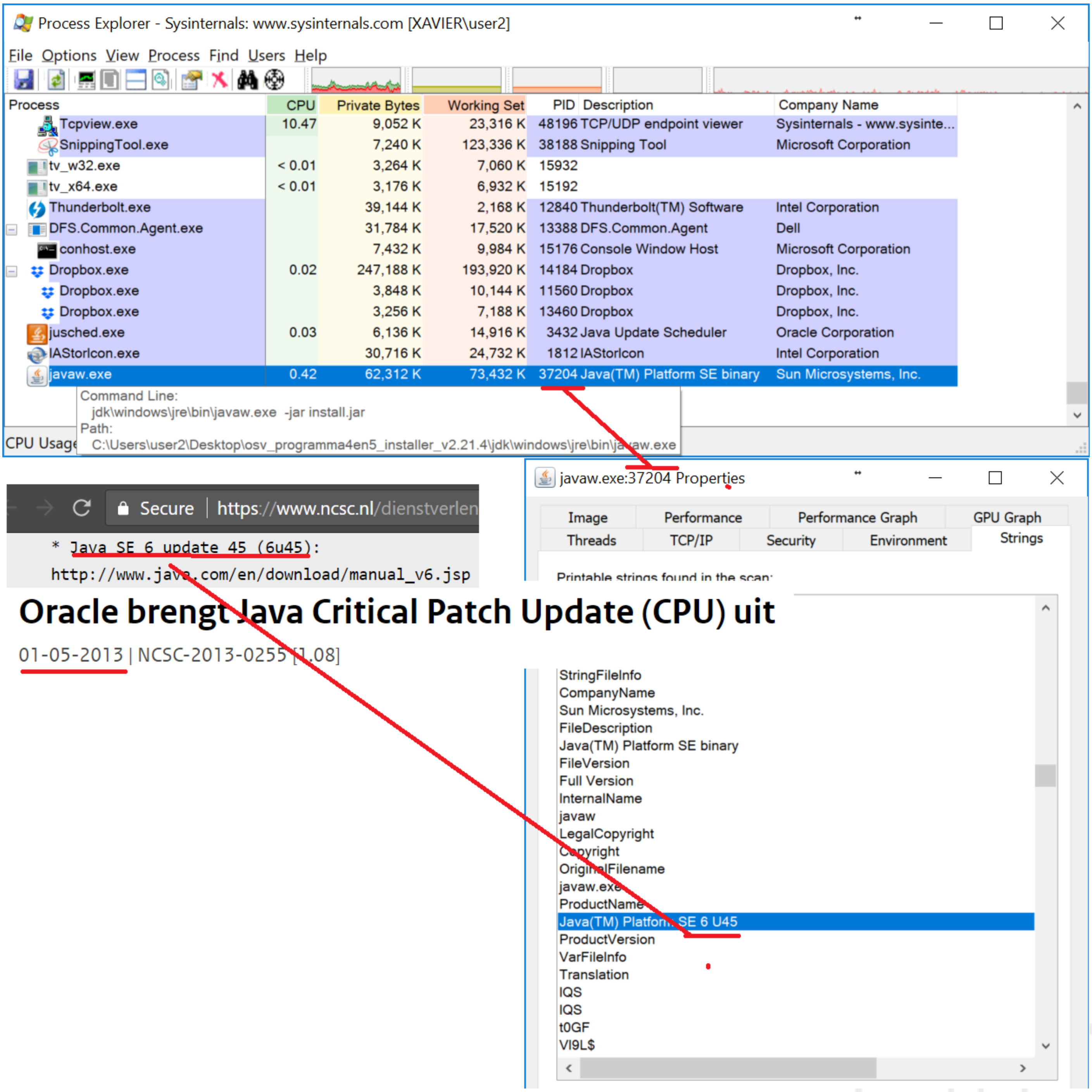
- *"[..] Een uitzondering hierop vormt de aanwezigheid van een 'poort' die via het netwerk benaderbaar is en niet direct noodzakelijk lijkt te zijn voor het correct functioneren van de oplossing. Binnen de beperkt beschikbare tijd heeft Fox-IT niet kunnen vaststellen of het mogelijk is om de software aan te vallen via deze poort. Daarnaast worden mogelijk onnodige TCP-poorten geopend op de OSV-server.*

  Op de OSV-server worden enkele poorten geopend die niet bereikbaar hoeven te zijn vanaf het netwerk, waaronder mogelijk poorten die RMI-toegang mogelijk maken. In verband met de beschikbare tijd heeft Fox-IT deze aanvalsvector niet verder onderzocht.

  Ongebruikte functionaliteit en/of onnodige bereikbaar poorten kan (onbekende) kwetsbaarheden onnodig blootstellen aan een mogelijke aanvaller. In het geval dat een kwetsbaarheid aangetroffen wordt zou dit, in het slechtste geval, kunnen leiden tot het compromitteren van de OSV-server. [..]"

4.1.4 High: Unsupported and old JBoss and Java SE software used

On the OSV server the file `\jboss-4.2.3.GA\readme.html` reveils that JBoss version `4.2.3GA` is used. This version was released 7.5 years ago on July 18, 2008. [23]


Process Explorer - Sysinternals: www.sysinternals.com [XAVIER\user2]
File Options View Process Find Users Help
CPU Usage
javaw.exe:37204 Properties
Image
Performance
Performance Graph
GPU Graph
Threads
TCP/IP
Security
Environment
Strings

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Tcpview.exe	10.47	9,052 K	23,316 K	48196	TCP/UDP endpoint viewer	Sysinternals - www.sysinte...
SnippingTool.exe		7,240 K	123,336 K	38188	Snipping Tool	Microsoft Corporation
tv_w32.exe	< 0.01	3,264 K	7,060 K	15932		
tv_x64.exe	< 0.01	3,176 K	6,932 K	15192		
Thunderbolt.exe		39,144 K	2,168 K	12840	Thunderbolt(TM) Software	Intel Corporation
DFS.Common.Agent.exe		31,784 K	17,520 K	13388	DFS.Common.Agent	Dell
conhost.exe		7,432 K	9,984 K	15176	Console Window Host	Microsoft Corporation
Dropbox.exe	0.02	247,188 K	193,920 K	14184	Dropbox	Dropbox, Inc.
Dropbox.exe		3,848 K	10,144 K	11560	Dropbox	Dropbox, Inc.
Dropbox.exe		3,256 K	7,188 K	13460	Dropbox	Dropbox, Inc.
jusched.exe	0.03	6,136 K	14,916 K	3432	Java Update Scheduler	Oracle Corporation
IAStorIcon.exe		30,716 K	24,732 K	1812	IAStorIcon	Intel Corporation
javaw.exe	0.42	62,312 K	73,432 K	37204	Java(TM) Platform SE binary	Sun Microsystems, Inc.

```
Command Line:
  jdk\windows\jre\bin\javaw.exe  -jar install.jar
Path:
  C:\Users\user2\Desktop\osv_programma4en5_installer_v2.21.4\jdk\windows\jre\bin\javaw.exe
```

Secure | https://www.ncsc.nl/dienstverlen

```
  * Java SE 6 update 45 (6u45):
  http://www.java.com/en/download/manual_v6.jsp
```

Oracle brengt Java Critical Patch Update (CPU) uit

01-05-2013 | NCSC-2013-0255 [1.08]

Printable strings found in the scan:

```
StringFileInfo
CompanyName
Sun Microsystems, Inc.
FileDescription
Java(TM) Platform SE binary
FileVersion
Full Version
InternalName
javaw
LegalCopyright
Copyright
OriginalFilename
javaw.exe
ProductName
Java(TM) Platform SE 6 U45
ProductVersion
VarFileInfo
Translation
IQS
IQS
t0GF
VI9L$
```

[23] See: http://jbossas.jboss.org/downloads

The file `/.installation files` reveals that Java SE version 1.6.0_45-b06t is used:

```
[..]
SYSTEM_java_runtime_version = 1.6.0_45-b06t
SYSTEM_java_runtime_namet = Java(TM) SE Runtime Environment FORCE64BIT
[..]
```

Runtime inspection of the OSV server with Process Explorer confirmed that Oracle Java SE version `1.6.0_45` is used:
This Java SE version is released almost 5 years ago on May 1, 2013. Oracle lists on their website the following update policy[24]:

- *"[..] updates for Java SE 6 released after April 2013 are only available to Oracle Customers through My Oracle Support (requires support login). [..]"*

Java SE version 9.0.4 is the latest version currently.

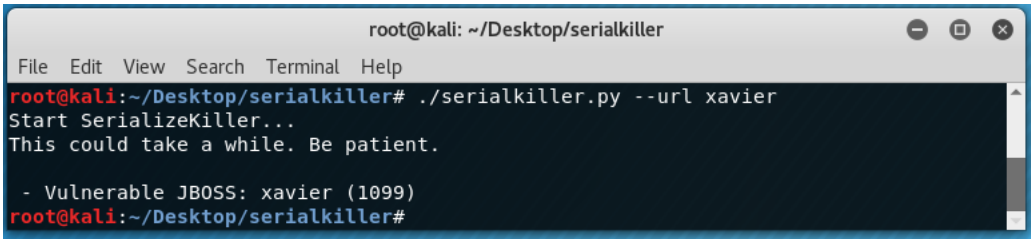
Impact

Both JBoss and Java SE are important components that OSV is build on. Important security updates are missing in both components.

Java is opening multiple ports unnecessary on the OSV server creating vulnerable attack surface for attackers that have gained access to the local OSV network (see also chapter 4.1.3):

```
nmap -sT -sV -p 1099,3648,3873,4444,8080,8083,8443 -O osv.local

PORT      STATE SERVICE     REASON  VERSION
1099/tcp  open  java-rmi    syn-ack Java RMI
3873/tcp  open  java-rmi    syn-ack Java RMI
4444/tcp  open  rmiregistry syn-ack Java RMI
8083/tcp  open  us-srv?     syn-ack
8443/tcp  open  ssl/http    syn-ack Apache Tomcat/Coyote JSP engine 1.1
```

Via these open ports with missing security patches the OSV server might be hackable via for example a Java deserialization attack[25]. To test if this was possible, the SerializeKiller Java deserialization vulnerability scanner from John de Kroon was run:

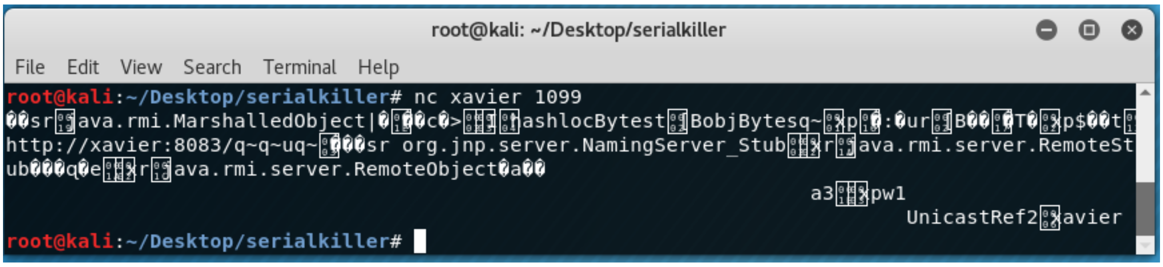

root@kali: ~/Desktop/serialkiller
File Edit View Search Terminal Help

```
root@kali:~/Desktop/serialkiller# ./serialkiller.py --url xavier
Start SerializeKiller...
This could take a while. Be patient.

 - Vulnerable JBOSS: xavier (1099)
root@kali:~/Desktop/serialkiller#
```

[24] See: http://www.oracle.com/technetwork/java/javase/downloads/index.html

[25] See: https://github.com/GrrrDog/Java-Deserialization-Cheat-Sheet/blob/master/README.md

Netcat confirms the Java RMI interface:


root@kali: ~/Desktop/serialkiller
File Edit View Search Terminal Help

```
root@kali:~/Desktop/serialkiller# nc xavier 1099
��sr□ava.rmi.MarshalledObject|�□��c�>□□□ashlocBytest□BobjBytesq~□xp□�:�ur□B��□�T�□xp$��t□
http://xavier:8083/q~q~uq~□���sr org.jnp.server.NamingServer_Stub□□xr□ava.rmi.server.RemoteSt
ub���q�e□□xr□ava.rmi.server.RemoteObject�a��
                                                                   a3□□xpw1
                                                                           UnicastRef2□xavier

root@kali:~/Desktop/serialkiller# 
```

The Java RMI interface on TCP port 1099 seems to be vulnerable for remote code execution via Java deserialization. Due to time constraints the actual exploitation of this vulnerability was not further researched.

The Fox-IT rapport from 2017 stated the following about the out-dated Java and JBoss software:

- *"[..] Het meest opvallende aan OSV vanuit een beveiligingsperspectief, is de sterk verouderde ondersteunende software waarop OSV draait. Dit is in ieder geval van toepassing op software componenten zoals de gebruikte Java-versie en de gebruikte Jboss-versie. Het gevolg hiervan is dat de software kwetsbaarheden kan bevatten die niet meer door de leverancier zullen worden opgelost en dat de software derhalve niet meer bijgewerkt kan worden met de laatst beschikbare beveiligingsmaatregelen. [..]"*

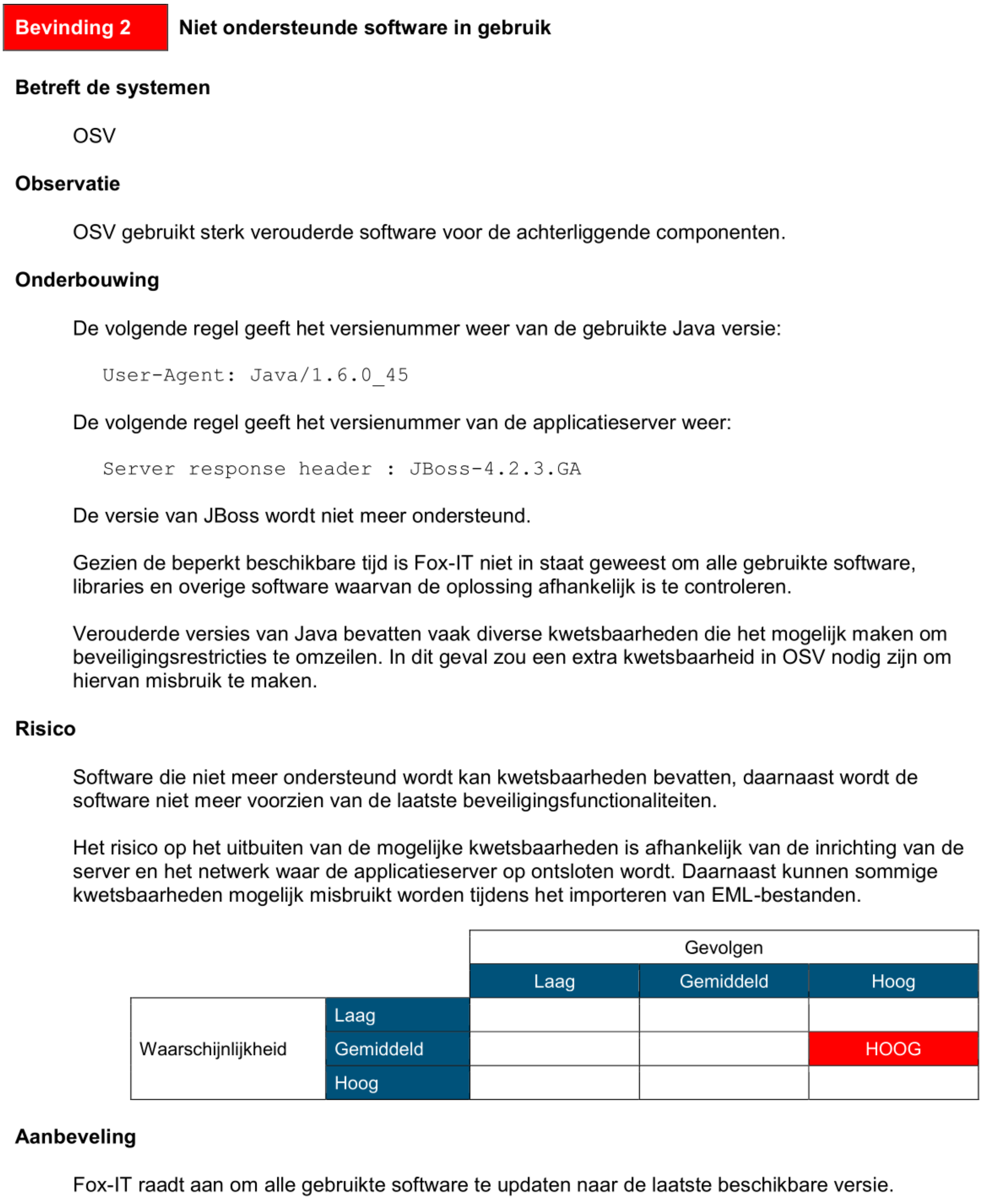
The SQS rapport from 2018 stated the following about out-dated software:

- *"[..]* ***Eis 5, de mate waarin technische mogelijkheden ter voorkoming van foutief gebruik worden uitgenut:***
  OSV gebruikt verouderde en/of niet meer ondersteunde softwarecomponenten zoals de gebruikte versies van Java en Jboss. Dit levert een beveiligingsrisico. De Kiesraad heeft organisatorische maatregelen genomen om dit technisch risico te mitigeren. [..] Als belangrijkste technische maatregel om verder foutief gebruik van OSV te voorkomen adviseren we om te onderzoeken of en hoe versies van gebruikte softwarecomponenten geactualiseerd kunnen worden. Dit verkleint de kans op misbruik van beveiligingslekken in deze componenten. [..]"

Recommendation

1. It is highly recommended to update all software components, and especially JBoss and Java SE to the latest version.
2. Close all unnecessary ports on the OSV server.

Additional text from the Fox IT report about the unsupported software that is used by OSV:



Bevinding 2 **Niet ondersteunde software in gebruik**

Betreft de systemen

OSV

Observatie

OSV gebruikt sterk verouderde software voor de achterliggende componenten.

Onderbouwing

De volgende regel geeft het versienummer weer van de gebruikte Java versie:

```
User-Agent: Java/1.6.0_45
```

De volgende regel geeft het versienummer van de applicatieserver weer:

```
Server response header : JBoss-4.2.3.GA
```

De versie van JBoss wordt niet meer ondersteund.

Gezien de beperkt beschikbare tijd is Fox-IT niet in staat geweest om alle gebruikte software, libraries en overige software waarvan de oplossing afhankelijk is te controleren.

Verouderde versies van Java bevatten vaak diverse kwetsbaarheden die het mogelijk maken om beveiligingsrestricties te omzeilen. In dit geval zou een extra kwetsbaarheid in OSV nodig zijn om hiervan misbruik te maken.

Risico

Software die niet meer ondersteund wordt kan kwetsbaarheden bevatten, daarnaast wordt de software niet meer voorzien van de laatste beveiligingsfunctionaliteiten.

Het risico op het uitbuiten van de mogelijke kwetsbaarheden is afhankelijk van de inrichting van de server en het netwerk waar de applicatieserver op ontsloten wordt. Daarnaast kunnen sommige kwetsbaarheden mogelijk misbruikt worden tijdens het importeren van EML-bestanden.

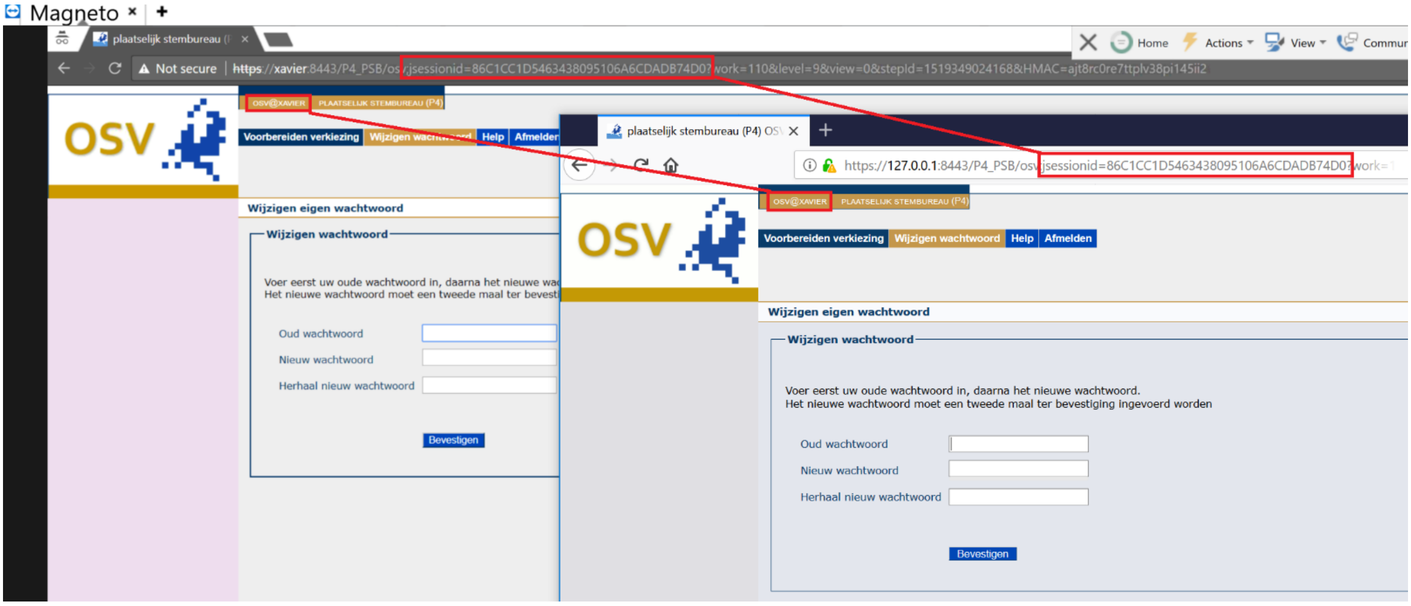
		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			
	Gemiddeld			HOOG
	Hoog			

Aanbeveling

Fox-IT raadt aan om alle gebruikte software te updaten naar de laatste beschikbare versie.

4.1.5 High: Lack of protection against session hijacking attacks

It is possible to be logged-in on user `osv` with two computers at the same time. A hacker that has access to the `jsessionid` token from another user that is logged-in on user `osv`, can use this token in his own browser to be also logged-in on user `osv`. The OSV server allows multiple computers to be logged-in on an user account.



https://xavier:8443/P4_PSB/osv;jsessionid=86C1CC1D5463438095106A6CDADB74D0?work=110&level=9&view=0&stepId=1519349024168&HMAC=ajt8rc0re7ttplv38pi145ii2

https://127.0.0.1:8443/P4_PSB/osv;jsessionid=86C1CC1D5463438095106A6CDADB74D0?work=

Voer eerst uw oude wachtwoord in, daarna het nieuwe wachtwoord.
Het nieuwe wachtwoord moet een tweede maal ter bevestiging ingevoerd worden

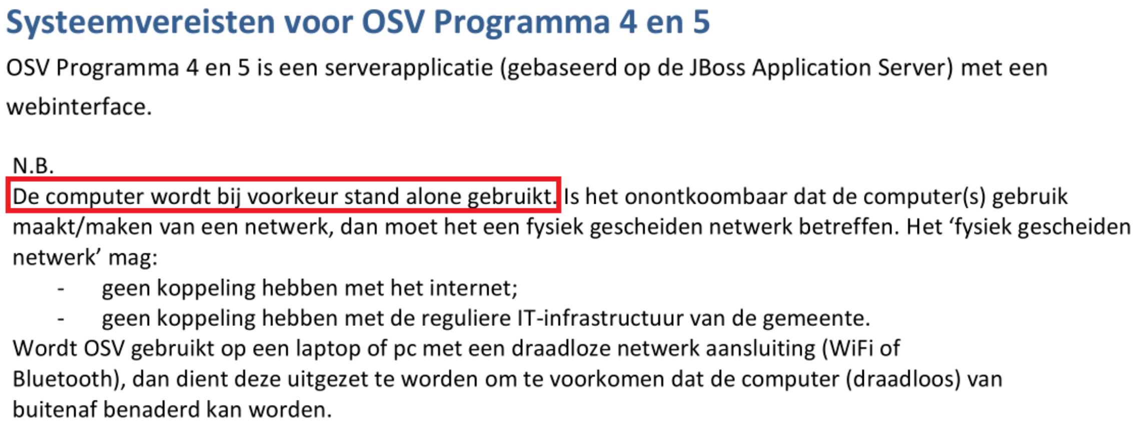
Risk :	High
Location :	`https://osv.local:8443/`
Description :	It is possible to be logged-in on user `osv` with two computers at the same time. A hacker that has access to the `jsessionid` token from another user that is logged-in on user `osv`, can use this token in his own browser to be also logged-in on user `osv`. The OSV server allows multiple computers to be logged-in on an user account.
Impact :	If the user has certain (exclusive) permissions to the computer, an attacker could exploit these authorizations when the session of the user is obtained.
Mitigated :	A session can not simply be hijacked. To achieve this, abusing another leak is necessary.
Recommendation :	1. Link a session to the IP address (and used user agent) of the user. Please note that this might also terminate legitimate sessions from mobile (roaming) users. 2. It is possible to create a fairly unique profile made up from the browser configuration (via JavaScript). A fairly unique id can be created looking at installed fonts and browser plugins, JavaScript version, browser information and much more.
Reproduction :	Log with Chrome into the OSV server with username `osv`. Afterwards copy the URL where the `jsessionid` token is visible in. Open OSV with another computer and IP address. Paste the URL in Firefox. It will result in that Chrome and Firefox are logged-in at the same time.
Patch status :	New

4.1.6 High: Four-eyes procedure can be circumvented by the second user

Risk :	High
Location :	`https://osv.local:8443/`
Description :	The Electoral Council publishes YouTube videos in which the functionality and processes around OSV are explained (in Dutch) towards end-users. In one of the videos the four-eyes procedure implemented in OSV is explained. The four-eyes procedure can be circumvented by the OSV user that will validate the input of the first user. The second OSV user is allowed to overwrite the input of the first user.
Impact :	The second OSV user that has to validate the total votes per political party submitted by the first user, can choose to ignore the votes
Recommendation :	Make sure that the second user cannot overwrite the input of the first user. The votes submitted by the first and second user should match exactly.
Evidence:	From 3:50 minutes in the YouTube video at https://www.youtube.com/watch?v=PUoBSQiKQWE the following is said by the instructor: • *"[..] Ter controle wordt voor de tweede invoer de N10 doorgegeven aan een tweede persoon. De eerste persoon verlaat het invoerscherm voor betreffend stembureau en gaat verder met een volgend stembureau. De tweede persoon ontvangt het doorgegeven procesverbaal, selecteert het betreffende stembureau op zijn eigen werkstation en gaat verder met het tweede invoer. De eerste invoer wordt nu niet getoond. De tweede persoon voert hier de aantallen in en slaat ook deze op. In het geval er verschillen gevonden wordt zullen deze in een geel warschuwingsvenster getoond worden. [..] bij verschillen wordt het volgende uitgangspunt toegepast: de tweede invoer is de definieve invoer. Om die reden keert u niet terug naar de eerste invoer als er verschillen tussen de 1e en 2e invoer worden geconstateerd. U zorgt er nu voor dat in elk veld waar een verschil getoond wordt het juiste getal komt te staan zoals dit op het procesverbaal N10 is aangegeven. Daarna klikt u op invoer bevestigen. Op dat moment wordt de invoer definitef en wordt ook de eerste invoer gecorrigeerd en komt er een donkergroen vinkteken links van het stembureau te staan. Er kan nu verder gegaan worden met een ander stembureau [..]"*
Patch status :	New

4.1.7 High: Stand-alone OSV installation is risky

The system requirements document about OSV program 4 and 5 states that the OSV should preferably run on a stand-alone computer[26]:



Systeemvereisten voor OSV Programma 4 en 5

OSV Programma 4 en 5 is een serverapplicatie (gebaseerd op de JBoss Application Server) met een webinterface.

N.B.
De computer wordt bij voorkeur stand alone gebruikt. Is het onontkoombaar dat de computer(s) gebruik maakt/maken van een netwerk, dan moet het een fysiek gescheiden netwerk betreffen. Het 'fysiek gescheiden netwerk' mag:

- geen koppeling hebben met het internet;
- geen koppeling hebben met de reguliere IT-infrastructuur van de gemeente.

Wordt OSV gebruikt op een laptop of pc met een draadloze netwerk aansluiting (WiFi of Bluetooth), dan dient deze uitgezet te worden om te voorkomen dat de computer (draadloos) van buitenaf benaderd kan worden.

Nowhere in the documentation is stated that each OSV user should work under a separated operating system user account.

Impact

1. If the OSV server is started under the same operating system user account as the OSV users will work under, then OSV users could access and change the Derby database OSV uses and directly manipulate votes stored in OSV (see chapter 4.1.2). They could also modify the OSV software.
2. If multiple OSV users are working under the same operating system user account, then one user could manipulate the computer and intercept login details from each user that will use the computer after him.

Recommendation

1. Start the OSV server under a different user than OSV users will work under on the same stand-alone computer.
2. Let each OSV user work under a different operating system user.

[26] See: https://www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/systeemvereisten-voor-osv-programma-4-en-5

4.1.8 Medium: Official vote reports from polling stations are not published on the internet

Currently it is up to each municipality to publish the vote totals of each polling station on their website. Some cities publish in their own format all the vote totals of a polling station, and others only publish the aggregated total votes in a municipality without details of all the vote totals of each polling station. Scans of each official paper polling station report (process-verbaal) are never uploaded to the internet. A digital export file of all the vote totals is generated by OSV, converted to HTML by municipalities and published (partially) on their website.

Impact
The official polling station reports that contain all the vote totals of a municipality can only be looked at offline at the office of a municipality. This raises the bar significantly for citizens and polling station chairmans to validate if someone has tampered with the election outcome in the totalization process. If a concerned citizen wants to independently validate all the totalizing of votes himself in The Netherlands, he or she would have to visit each municipality and copy all the official reports from polling stations. This takes a lot of time. Elections should be completely verifiable with minimal effort by everyone that thinks election integrity is at risk.

Recommendation
Complete transparency and easy access of official vote reports from polling stations. It is strongly advised to immediately scan all official vote total reports (processen-verbalen) from polling stations and upload them to a secure portal a couple of days after elections are held. This portal does not currently exist and should be developed by the Central Electoral council. This portal should also also publish all uploaded official vote totals reports on their website so people can independently review them.

Risk rating
Medium

Status
In a reaction the Electoral Council states towards RTL News that: *"A bill is being prepared in which all official reports from polling stations will be made public on the internet in the future."*. Good to hear this point is already being picked up!

4.1.9 Medium: Hack attacks aren't detected as an intrusion detection system is missing

The OSV server does not block and detect hacking attacks. A custom made intrusion detection and prevention system is missing. See also the security risks described in chapter 4.1.2, 4.1.10, 4.1.15 and 4.1.18.

4.1.10 Medium: Integrity of OSV software is only checked when installing it

The integrity of OSV software is only checked when initially installing it.

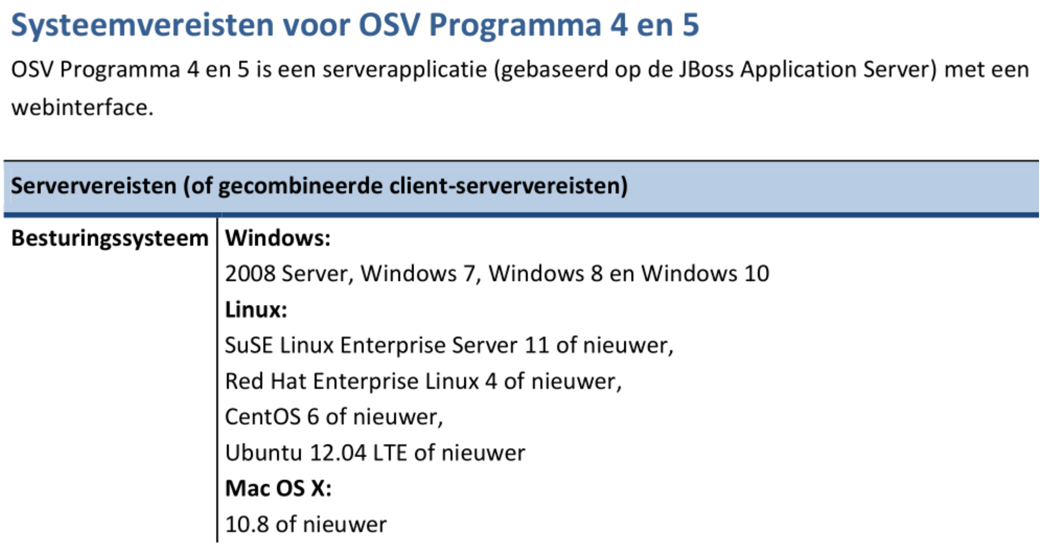
Impact
No integrity checks are performed by OSV itself to check if it has been manipulated.

Recommendation
Let OSV continuously monitor the integrity of the OSV server installation and files that OSV generated. Encrypt the Derby database and XML/EML files with a custom password per OSV installation.

4.1.11 Medium: Any server will do

The Electoral Council has provided municipalities security instructions and documentations on how to properly and securely install OSV on. OSV can be installed on Windows, Linux and MacOS. The municipality will have to install and configure the operating system OSV runs on.

The minimal system requirements for the OSV server are[27]:



Systeemvereisten voor OSV Programma 4 en 5

OSV Programma 4 en 5 is een serverapplicatie (gebaseerd op de JBoss Application Server) met een webinterface.

Serververeisten (of gecombineerde client-serververeisten)	
Besturingssysteem	**Windows:** 2008 Server, Windows 7, Windows 8 en Windows 10 **Linux:** SuSE Linux Enterprise Server 11 of nieuwer, Red Hat Enterprise Linux 4 of nieuwer, CentOS 6 of nieuwer, Ubuntu 12.04 LTE of nieuwer **Mac OS X:** 10.8 of nieuwer

Impact

From a security point of view it is always recommended to use the latest available version of a software package, even if no security patch is missing according to the release documentation. Some software vendors choose to silently patch vulnerabilities.

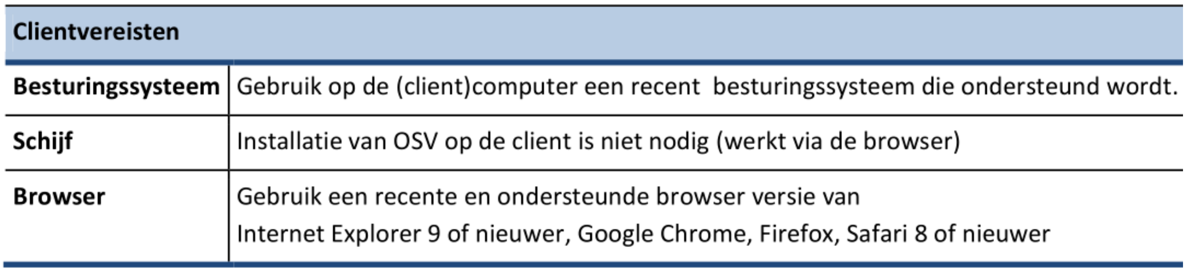
Recommendation

The Kiesraad should supply a CD-ROM file with a hardened and minimized open source Linux distribution on it. The Linux installation should have the OSV server pre-installed on it. This way there is full control over the operating system that the OSV server runs on. Disallow Windows and Mac OS X servers.

[27] See: https://www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/systeemvereisten-voor-osv-programma-4-en-5

4.1.12 Medium: Any browser will do

The minimal system requirements for the OSV clients are[28]:



Clientvereisten	
Besturingssysteem	Gebruik op de (client)computer een recent besturingssysteem die ondersteund wordt.
Schijf	Installatie van OSV op de client is niet nodig (werkt via de browser)
Browser	Gebruik een recente en ondersteunde browser versie van Internet Explorer 9 of nieuwer, Google Chrome, Firefox, Safari 8 of nieuwer

The OSV server allows any browser. Even old-dated, insecure and unsupported browsers. In the OSV installation manual system administrators are instructed to use a recent and supported browser version. They are not instructed to use the latest version of a browser.

Impact
From a security point of view it is always recommended to use the latest available version of a software package, even if no security patch is missing according to the release documentation. Some software vendors choose to silently patch vulnerabilities.

Recommendation
Inspect server-side the `User-Agent` HTTP header that client browsers sent to the OSV server. Detect which browser version is used to access the OSV server. Block outdated and insecure browsers.

[28] See: https://www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/systeemvereisten-voor-osv-programma-4-en-5

4.1.13 Medium: Session token inside URL

Risk :	Medium
Hostname :	`osv.local`
Location :	`https://osv.local:8443/P4_PSB/osv/wahl/refresh;jsessionid=86C1CC1D5463438095106A6CDADB74D0?work=138&level=9&view=0&stepId=1519349128854&HMAC=9q4iyqf0d77ish4bwjfhkbn23`
Description :	When an user logs into OSV, the web server gives the user's browser an unique session token so that it knows that the user is logged-in. The session token is transferred to the server via the `jsessionid` GET variable.
Impact :	This configuration makes identity theft in certain cases possible via session hijacking. When session identifier tokens are in the URL, then these have a lower level of trust than if these are only transmitted via HTTP headers: 1. If the session token is in the URL, then this can be read with JavaScript (even if the token is normally protected by `HttpOnly` protection on the session cookie). 2. When a user clicks on a link that refers to another website, then the browser sends the session token with the `Referer` HTTP header to the other website. System administrators of that website can then access the session token. 3. When a user does not log out of the application, but for example just closes the browser before walking away from the computer, then a malicious person could look up the browser history and click on a link to the application in which still a valid token is listed. In that case the victim is still logged on into the application and this can be exploited by a malicious person. 4. A user of the application can copy the URL and send that to a third party in order to share the link to the application. It is likely that the user is unaware that this will allow the receiving person to be logged in as the person who sent the link.
Mitigated :	A session token expires two minutes after it is not used anymore.
Recommendation :	Configure the communication between the server and the client in such a way, that session ID tokens are exchanged only via cookies (which are protected by the `HttpOnly`, `Secure` and `SameSite` option).

Reproduction :	`GET /P4_PSB/osv/wahl/refresh;jsessionid=86C1CC1D5463438095106A6CDADB74D0?work=138&level=9&view=0&stepId=1519349128854&HMAC=9q4iyqf0d77ish4bwjfhkbn23 HTTP/1.1`
	`Host: osv.local:8443`

Patch status :	Open (not solved)

The Fox IT report states:

- *"[..] De OSV-webapplicatie geeft het sessie-id van de gebruiker weer in de URL en stuurt deze bij elk verzoek van de browser terug naar de server. [..] Het weergeven van het sessie-id in de URL kan ervoor zorgen dat een aanvaller met fysieke toegang tot een OSV-client in staat is om het sessie-id over te nemen, waarmee de sessie gekaapt zou kunnen worden. [..]"*

4.1.14 Medium: SSL version 3.0 is detected

Risk :	Medium
Hostname :	`osv.local`
Location :	`https://osv.local:8443/`
Description :	SSL version 3 is used.
Impact :	An attacker with access to the network traffic between the server and a client may be able to decrypt captured encrypted traffic. SSL version 3 is vulnerable for the POODLE attack via which session cookies can be decrypted in certain circumstances, which can lead to identity theft via a man-in-the-middle attack.
Recommendation :	1. Allow only TLS version 1.2 with only the `AEAD` cipher suite. Perform a thorough functional test to check if all legitimate users of the secure connection support this protocol and algorithm. 2. Disable SSL version 3.
Patch status :	New
Website :	1. Qualys: SSL/TLS deployment best practices 2. Qualys: SSL 3 is dead, killed by the POODLE attack 3. This POODLE bites: exploiting the SSL 3.0 fallback 4. The POODLE Attack and the End of SSL 3.0 5. Strong SSL/TLS Cryptography in Apache and Nginx 6. CVE-2014-3566 7. How to disable SSLv3 8. How POODLE Happened 9. This POODLE bites: exploiting the SSL 3.0 fallback (technical paper)

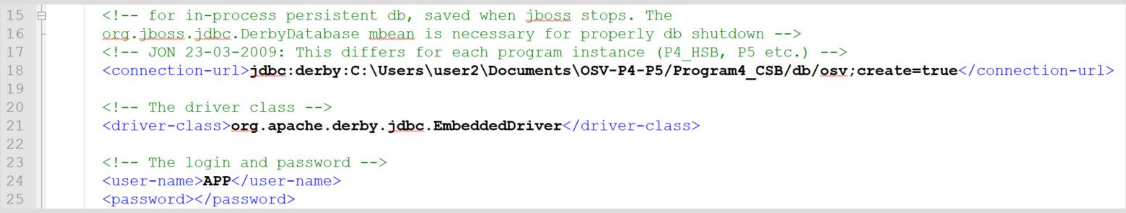
4.1.15 Medium: The OSV servers keeps running even if an internet connection is present

The OSV servers keeps running even if an internet connection is available.

Recommendations

1. Don't allow the OSV server to run if an internet connection is detected and display a security notification.
2. Sent a security incident report of the matter to the security mailbox of Electoral Council and IVU.
3. If a production OSV server from a municipality is connected to the internet during election time, alarms should go off.

4.1.16 Medium: OSV database isn't protected by a password

Risk :	Medium
Location :	On osv.local: /Program4_CSB/db/osv;create=true /Program4_HSB/db/osv /Program4_PSB/db/osv /Program4_PSB_2/db/osv /Program4_PSB_3/db/osv /Program4_PSB_4/db/osv /Program4_PSB_5/db/osv /Program5/db/osv
Description :	The Derby database that OSV used has not password configured. OSV logs in with username APP and no password. The same database user account is also used for P4 and P5.
Impact :	An attacker can gain easily gain access to the system by guessing the password.
Recommendation :	Configure a strong password for the OSV Derby database. Make sure that the password and username is different for each OSV installation. Also implement a separate database user for P4 and P5.
Evidence :	The file \jboss-4.2.3.GA\server\osv\deploy\derby-ds.xml contains the database login credentials of the Derby database server that is used:  <!-- for in-process persistent db, saved when jboss stops. The org.jboss.jdbc.DerbyDatabase mbean is necessary for properly db shutdown --> <!-- JON 23-03-2009: This differs for each program instance (P4_HSB, P5 etc.) --> <connection-url>jdbc:derby:C:\Users\user2\Documents\OSV-P4-P5/Program4_CSB/db/osv;create=true</connection-url> <!-- The driver class --> <driver-class>org.apache.derby.jdbc.EmbeddedDriver</driver-class> <!-- The login and password --> <user-name>APP</user-name> <password></password> [..] <local-tx-datasource> <connection-url>jdbc:derby:C:\Users\testuser\Documents\OSV-P4-P5/Program4_CSB/db/osv;create=true</connection-url> [..] <user-name>APP</user-name> <password></password> [..] </local-tx-datasource> <local-tx-datasource> <connection-url>jdbc:derby:C:\Users\testuser\Documents\OSV-P4-P5/Program4_HSB/db/osv;create=true</connection-url> [..] <user-name>APP</user-name> <password></password> </local-tx-datasource> [..] <local-tx-datasource> <connection-url>jdbc:derby:C:\Users\testuser\Documents\OSV-P4-P5/Program4_PSB/db/osv;create=true</connection-url> [..] <user-name>APP</user-name> <password></password> [..] </local-tx-datasource> <local-tx-datasource> <connection-url>jdbc:derby:C:\Users\testuser\Documents\OSV-P4-P5/Program4_PSB_2/db/osv;create=true</connection-url> [..] <user-name>APP</user-name> <password></password> [..] </local-tx-datasource> <local-tx-datasource> <connection-url>jdbc:derby:C:\Users\testuser\Documents\OSV-P4-P5/Program4_PSB_3/db/osv;create=true</connection-url> [..] <user-name>APP</user-name>

	<password></password> [..] </local-tx-datasource> <local-tx-datasource> <connection-url>jdbc:derby:C:\Users\testuser\Documents\OSV-P4-P5/Program4_PSB_4/db/osv;create=true</connection-url> [..] <user-name>APP</user-name> <password></password> [..] </local-tx-datasource> <local-tx-datasource> <connection-url>jdbc:derby:C:\Users\testuser\Documents\OSV-P4-P5/Program4_PSB_5/db/osv;create=true</connection-url> [..] <user-name>APP</user-name> <password></password> [..] </local-tx-datasource> <local-tx-datasource> <connection-url>jdbc:derby:C:\Users\testuser\Documents\OSV-P4-P5/Program5/db/osv;create=true</connection-url> [..] <user-name>APP</user-name> <password></password> [..] </local-tx-datasource> [..]
Patch status :	New

4.1.17 Medium: Election results (EML files) should be e-mailed to the Electoral Council

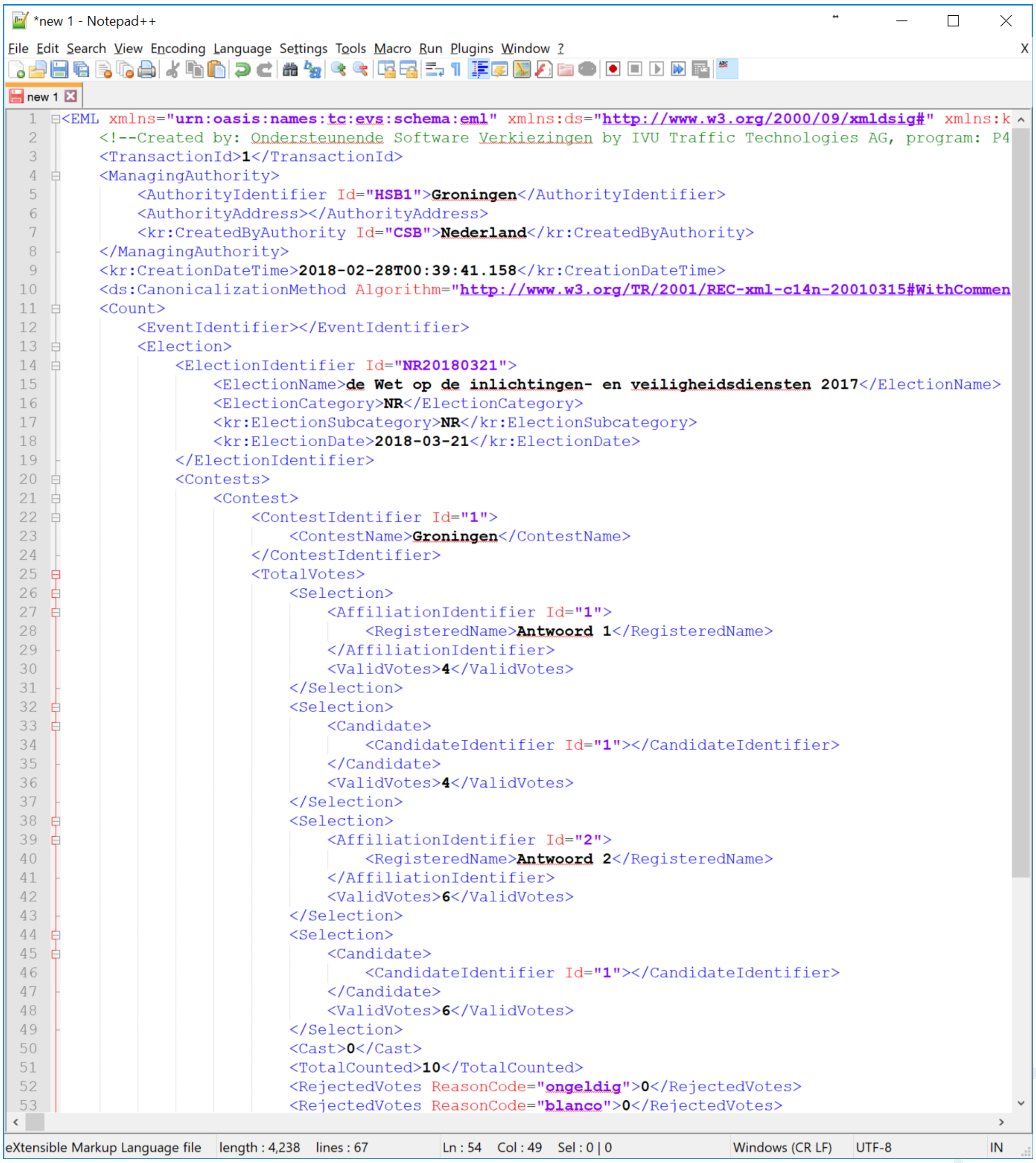
Risk :	Medium
Hostname :	City internal network
Location :	SMTP servers used in the chain towards the SMTP server of Kiesraad.
Description :	The EML files OSV generates have to be mailed to the Kiesraad. E-mail are sent unencrypted over the internet and are susceptible for manipulation via a man-in-the-middle attack.
Impact :	When an attacker has access to communication between the client and the server, various attack scenarios are possible: 1. Confidential information such as authentication information (passwords) and personal data may be intercepted. This makes identity theft possible. 2. Visitors to the legitimate service (such as a website) can be sent to an almost identical looking, but malicious (*phishing*) service, without the user noticing. 3. The content of the communication can be modified, allowing for example incorrect information to be displayed.
Recommendation :	Create a secure EML upload portal with an encrypted HTTPS connection where OSV users can securely upload EML files towards the Kiesraad. For example, via `https://osv.kiesraad.nl/`. This is a much better alternative than sending files unauthenticated and unencrypted via e-mail.
Patch status :	Open (not solved)
Website :	Wikipedia.org: Transport Layer Security

4.1.18 Medium: Modified EML files in archive directory on the server aren't detected

OSV generates EML files on the server that can be downloaded to be processed by the OSV user. If an EML file that OSV generated is modified on the server by a hacker, then OSV will not detect this. OSV does not perform integrity checks on anything. OSV assumes that it won't get hacked and thus won't check if generated EML files are manually modified later on.

Impact

It was possible to change votes in the EML file that OSV generated. The modified EML file could be downloaded via the OSV export directory in the interface on https://osv.local:8443/. OSV did not detect the modified EML file.


*new 1 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 1

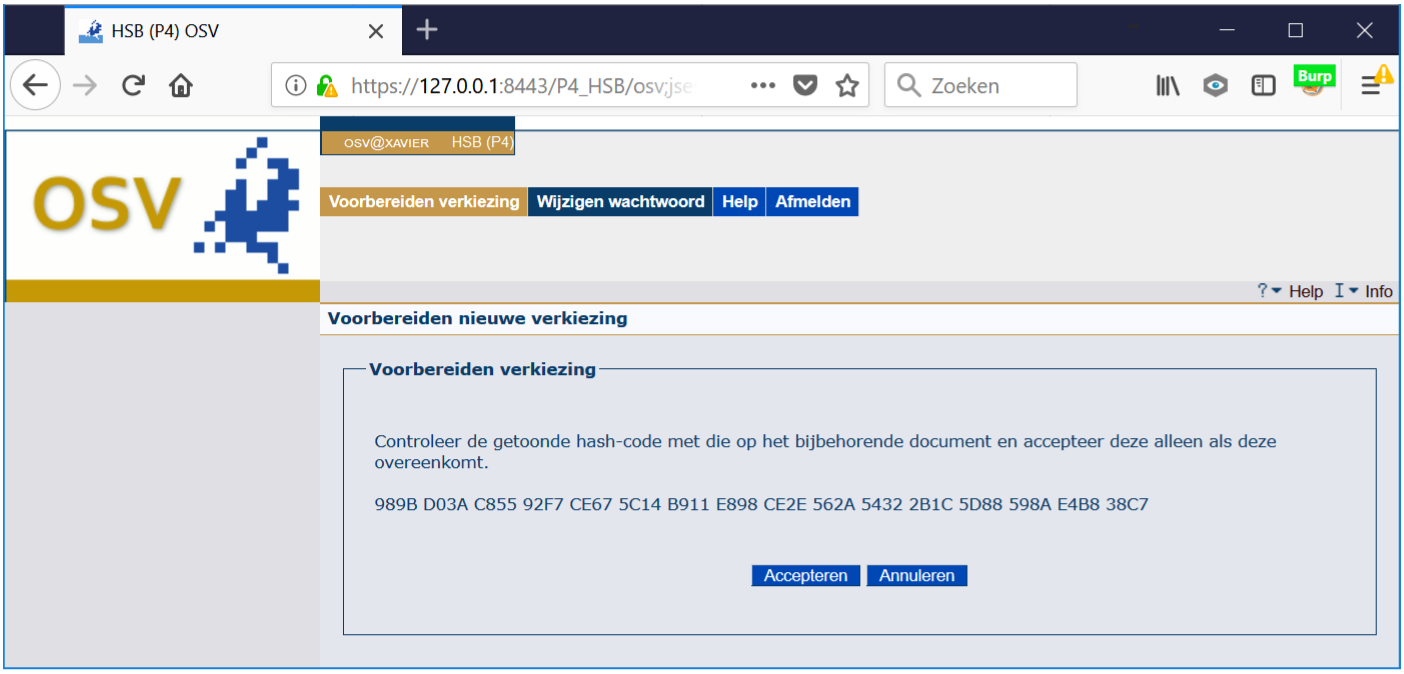
```
<EML xmlns="urn:oasis:names:tc:evs:schema:eml" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:k
    <!--Created by: Ondersteunende Software Verkiezingen by IVU Traffic Technologies AG, program: P4
    <TransactionId>1</TransactionId>
    <ManagingAuthority>
        <AuthorityIdentifier Id="HSB1">Groningen</AuthorityIdentifier>
        <AuthorityAddress></AuthorityAddress>
        <kr:CreatedByAuthority Id="CSB">Nederland</kr:CreatedByAuthority>
    </ManagingAuthority>
    <kr:CreationDateTime>2018-02-28T00:39:41.158</kr:CreationDateTime>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithCommen
    <Count>
        <EventIdentifier></EventIdentifier>
        <Election>
            <ElectionIdentifier Id="NR20180321">
                <ElectionName>de Wet op de inlichtingen- en veiligheidsdiensten 2017</ElectionName>
                <ElectionCategory>NR</ElectionCategory>
                <kr:ElectionSubcategory>NR</kr:ElectionSubcategory>
                <kr:ElectionDate>2018-03-21</kr:ElectionDate>
            </ElectionIdentifier>
            <Contests>
                <Contest>
                    <ContestIdentifier Id="1">
                        <ContestName>Groningen</ContestName>
                    </ContestIdentifier>
                    <TotalVotes>
                        <Selection>
                            <AffiliationIdentifier Id="1">
                                <RegisteredName>Antwoord 1</RegisteredName>
                            </AffiliationIdentifier>
                            <ValidVotes>4</ValidVotes>
                        </Selection>
                        <Selection>
                            <Candidate>
                                <CandidateIdentifier Id="1"></CandidateIdentifier>
                            </Candidate>
                            <ValidVotes>4</ValidVotes>
                        </Selection>
                        <Selection>
                            <AffiliationIdentifier Id="2">
                                <RegisteredName>Antwoord 2</RegisteredName>
                            </AffiliationIdentifier>
                            <ValidVotes>6</ValidVotes>
                        </Selection>
                        <Selection>
                            <Candidate>
                                <CandidateIdentifier Id="1"></CandidateIdentifier>
                            </Candidate>
                            <ValidVotes>6</ValidVotes>
                        </Selection>
                        <Cast>0</Cast>
                        <TotalCounted>10</TotalCounted>
                        <RejectedVotes ReasonCode="ongeldig">0</RejectedVotes>
                        <RejectedVotes ReasonCode="blanco">0</RejectedVotes>
```

Recommendation

OSV should continuously perform integrity check if anything important is maliciously modified and notify the OSV administrator on irregularities.

4.1.19 Medium: SHA256 code validation can be skipped in some cases

When importing EML files in OSV that contain the election definition, OSV displays a SHA256 checksum of the imported file. The user has to manual verify if the checksum corresponds with the official checksum. This validation can be easily skipped as the *'accepteren'* button can be pressed immediately. If an EML election definition is loaded and if the *'accepteren'* button is immediately pressed after the file was selected and loaded, and thus obviously took no time to check the hashcode, OSV software will accept this risky behavior.



Voorbereiden nieuwe verkiezing

Voorbereiden verkiezing

Controleer de getoonde hash-code met die op het bijbehorende document en accepteer deze alleen als deze overeenkomt.

989B D03A C855 92F7 CE67 5C14 B911 E898 CE2E 562A 5432 2B1C 5D88 598A E4B8 38C7

Risk

OSV users can easily skip the important SHA256 check.

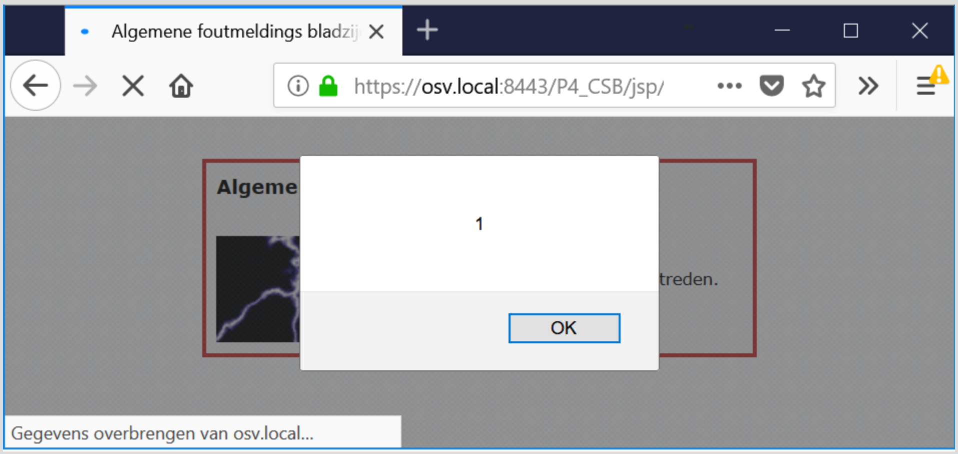
Recommendation

The user should type in the complete SHA256 code in OSV. This SHA256 could should not be displayed to the user. Only if the supplied SHA256 code by the user matches the hashcode OSV generated by itself, the EML file should be loaded.

4.1.20 Medium: Cross-site scripting is possible

Risk :	Medium
Hostname :	`osv.local`
Location :	`https://osv.local:8443/P4_CSB/jsp/wahl/login_dialog.jsp` `https://osv.local:8443/P4_PSB/osv`
Description :	It is possible to inject JavaScript into HTML code. Via this method, cross-site scripting (XSS) is possible. User input is not checked whether it contains the correct value and/or user input is not transformed into the right encoding when it is displayed.
Impact :	1. With a cross-site scripting attack it is for example possible to copy session cookies from other users. This enables session hijacking, allowing an attacker in certain circumstances to take over an (administrator) account. 2. The appearance of the website can be defaced, which can cause reputation damage. 3. Malicious software can be injected into the website.
Mitigated :	When a cross-site scripting vulnerability is abused by injection a payload into a web address, browsers often have a built-in protection against this kind of attack: 1. When an Internet address is opened in Internet Explorer 8 where JavaScript code is included in the web address, then the malicious code will automatically be converted into a harmless version. Also, the following message will be displayed: *"Internet Explorer has modified this page to help prevent cross-site scripting. Click here for more information ..."*. 2. When such an address is opened in Chrome version 8, Opera version 11 or Firefox version 3.6, then the malicious code will automatically be converted into a URL encoded variant, so the code will not be executed in the browser. 3. When the NoScript add-on is installed in Firefox, the code is harmless and the following message will be displayed: *"NoScript filtered a potential cross-site scripting (XSS) attempt from [http:// ...]. Technical details have logged to into the console."*.
Recommendation :	1. Make sure that the HTML code cannot be modified via user input. 2. When user input will be displayed, make sure that the input can never change the HTML structure. Make sure that you convert the following characters to the corresponding HTML entity variant: `< > " ' # & \r \n : ; ) ( /`. This conversion is a security measure against a lot of XSS variants, but not all. 3. Explicitly check all user input to make sure that it contains the correct values, for example by using white lists, and that these values are submitted in the correct format, for example a valid e-mail address. Make sure that people with malicious intent can't make injections into user input and that only trusted values will be accepted. The best security solution is to choose for an architectural approach, one that enforces that all controls will be executed, and that a check on user input could never be forgotten. Check if more vulnerabilities of this type occur in the software.
Evidence :	A blackbox reflected XSS: `https://osv.local:8443/P4_CSB/jsp/wahl/login_dialog.jsp;jsessionid=2ADE508C32A6F4A67C0101DF1526DB40?cmd=%3Cscript%3Ealert(1)%3C/script%3E`

```
GET
/P4_CSB/jsp/wahl/login_dialog.jsp;jsessionid=2ADE508C32A6F4A67C0101D
F1526DB40?cmd=%3Cscript%3Ealert(1)%3C/script%3E HTTP/1.1
Host: osv.local:8443

HTTP/1.1 500 Internal Server Error [..]
Content-Type: text/html;charset=ISO-8859-1

[..]
java.lang.RuntimeException: Command <script>alert(1)</script>
unknown at
de.ivu.wahl.client.beans.ApplicationBean.executeCommand(ApplicationB
ean.java:317) at
org.apache.jsp.jsp.wahl.login_005fdialog_jsp._jspService(login_005fd
ialog_jsp.java:157) at
org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
[..]
```


Algemene foutmeldings bladzij
https://osv.local:8443/P4_CSB/jsp/
Algeme
1
OK
treden.
Gegevens overbrengen van osv.local...

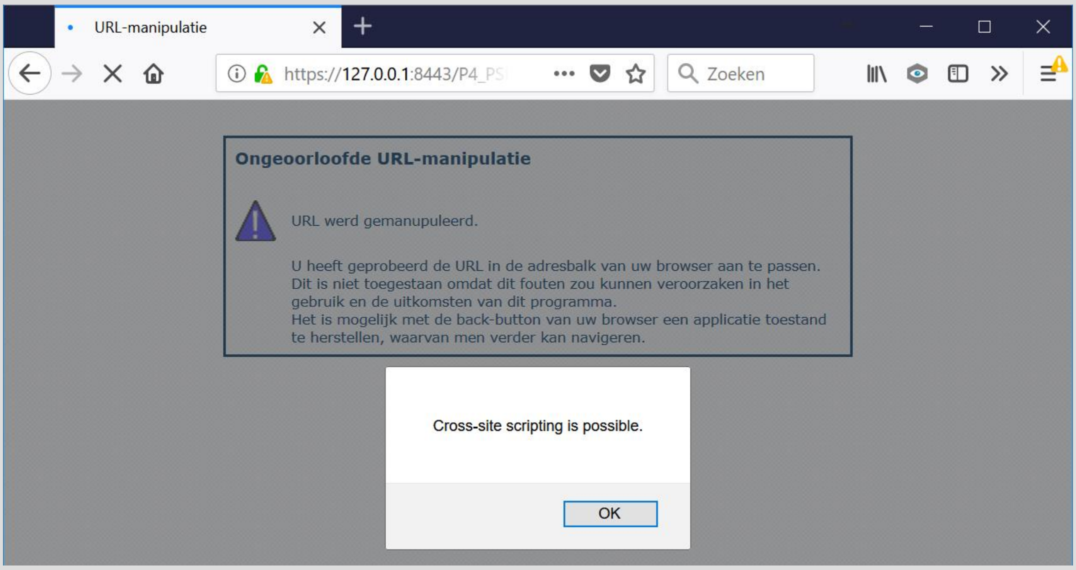
A greybox XSS:

```
GET /P4_PSB/osv;jsessionid=86C1CC1D5463438095106A6CDADB74D0?
view='%3e%3cscript%3ealert(1)%3c%2fscript%3e&level=9&work=138&stepId
=1519349024168&HMAC=5hekn1rtkpijecfer02wmh9m5 HTTP/1.1
Host: osv.local:8443
```

The OSV server responds by sending the following HTML code to the browser:

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=ISO-8859-1

[..]
U heeft geprobeerd de URL in de adresbalk van uw browser aan te
passen. Dit is niet toegestaan omdat dit fouten zou kunnen
veroorzaken in het gebruik en de uitkomsten van dit programma.<br />
Het is mogelijk met de back-button van uw browser een applicatie
toestand te herstellen, waarvan men verder kan navigeren.<br />
<a
href='/P4_PSB/osv;jsessionid=86C1CC1D5463438095106A6CDADB74D0?view='
><script>alert(1)</script>&amp;level=0&amp;work=6&amp;stepId=1519349
024168&amp;HMAC=2tsefsbrgd60u3zsp0e7my6yp' target='_top'>Navigeer
hier verder als een applicatie toestand verloren kan gaan.
[..]
```

This results in the JavaScript payload in the URL to be executed in Firefox:



Ongeoorloofde URL-manipulatie

URL werd gemanupuleerd.

U heeft geprobeerd de URL in de adresbalk van uw browser aan te passen.
Dit is niet toegestaan omdat dit fouten zou kunnen veroorzaken in het gebruik en de uitkomsten van dit programma.
Het is mogelijk met de back-button van uw browser een applicatie toestand te herstellen, waarvan men verder kan navigeren.

Cross-site scripting is possible.

The responsible JSP file for this XSS leak is a page that is shown when an user has manipulated the URL. Ironically this page introduces a XSS leak by itself:

```
\osv45_v2.21.4_source_for_publication\osv45\websrc\jsp\UserManipulatedURL.js
p

[..]
<title><ivu:int key="URL_Manipulation.1"/></title> [..]
<%
      String url = "/osv?"+ClientHelper.getSuffixLevel(request,
ApplicationBeanKonstanten.LEVEL_INITIAL)+

"&"+ApplicationBeanKonstanten.WORKIS+ApplicationBeanKonstanten.GEB_ERG;
       %>
      <ivu:int key="URL_Manipulation.4"/><br />
      <ivu:int key="URL_Manipulation.5"/><br />
      <ivu:a href='<%=url%>'><ivu:int key="URL_Manipulation.6"/></ivu:a>
[..]
```

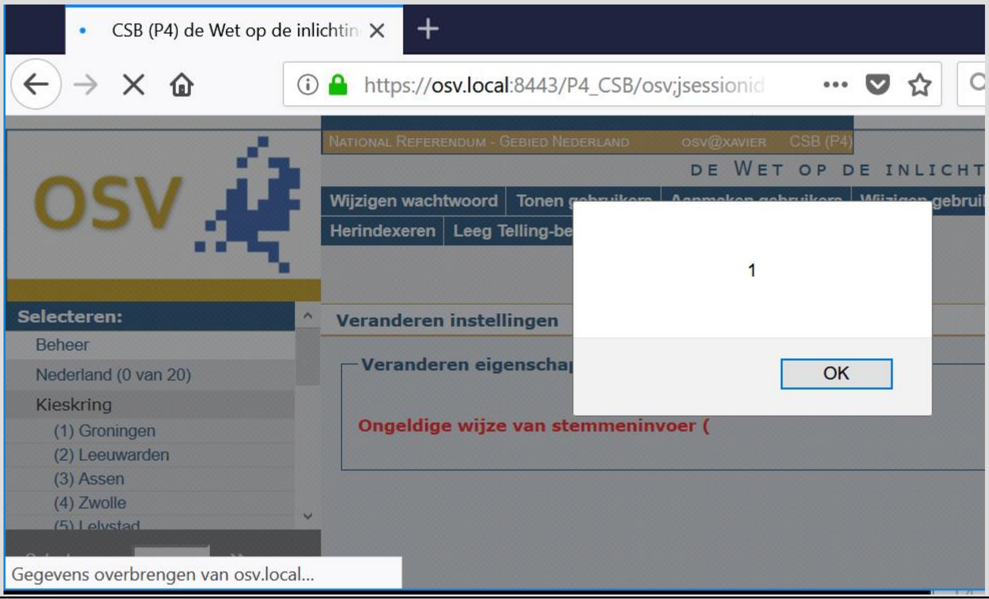
Another greybox XSS:

```
https://osv.local:8443/P4_CSB/osv;jsessionid=C389E09AED07309BF580921
3B3C4955D?cmd=adm_propEingabe&pre_subwork=0&work=122&level=9&view=0&
stepId=1519774249234&HMAC=b034an480o2lbismu2y8cy807

POST
/P4_CSB/osv;jsessionid=C389E09AED07309BF5809213B3C4955D?cmd=adm_prop
Eingabe&pre_subwork=0&work=122&level=9&view=0&stepId=1519774249234&H
MAC=b034an480o2lbismu2y8cy807 HTTP/1.1
Host: osv.local:8443
Referer:
https://osv.local:8443/P4_CSB/osv/wahl/arbeit;jsessionid=C389E09AED0
7309BF5809213B3C4955D?work=122&level=9&view=0&stepId=1519774249234&H
MAC=em6qiiupmx4dr07x3zgjz297y
Content-Type: application/x-www-form-urlencoded
Content-Length: 86
```

```
pre_DOUBLE_INPUT=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&pre_propueb
ernehmen=Overnemen
```

To view the injected JavaScript payload, the following URL should be called:

```
https://osv.local:8443/P4_CSB/osv/wahl/arbeit;jsessionid=C389E09AED0
7309BF5809213B3C4955D?work=122&level=9&view=0&stepId=1519774297376&H
MAC=25c93iywh9gj5000uupcme9lm

GET
/P4_CSB/osv/wahl/arbeit;jsessionid=C389E09AED07309BF5809213B3C4955D?
work=122&level=9&view=0&stepId=1519774297376&HMAC=25c93iywh9gj5000uu
pcme9lm HTTP/1.1
Host: osv.local:8443

HTTP/1.1 200 OK [..]
Content-Type: text/html;charset=UTF-8
[..]
Ongeldige wijze van stemmeninvoer (<script>alert(1)</script>).
Wijzig de waarde voor de invoer in 1, 2 of 3. [..]
```



1

Ongeldige wijze van stemmeninvoer (

Patch status : New

Website :

1. XSS cheat sheet
2. Wikipedia.org: XSS
3. WebAppSec.org on XSS
4. OWASP on XSS
5. Wikipedia: cross-site scripting

4.1.21 Medium: Browser back button works even if user is logged out (HTML code can be cached)

Risk :	Low
Hostname :	`osv.local`

Location :	`https://osv.local:8443 :`
	
	`/P4_CSB/osv/wahl/adm_anwender_change_pw_First;jsessionid=610B7EF2E3F246E9503EE440C5AD6699`
	`/P4_HSB-export-map/`
	`/P4_HSB-export-map/Telling_GR2017_MiddenGroningen_kieskring_MiddenGroningen_leeg.eml.xml`
	`/P4_HSB-export-map/archive/`
	`/P4_HSB-export-map/archive/Kandidatenlijsten_GR2017_MiddenGroningen.eml.xml`
	`/P4_HSB/osv/wahl/Info;jsessionid=09CEC0DADFEA1FF7CAF40B4A1E74A815`
	`/P4_HSB/osv/wahl/arbeit;jsessionid=09CEC0DADFEA1FF7CAF40B4A1E74A815`
	`/P4_HSB/osv/wahl/befehl;jsessionid=09CEC0DADFEA1FF7CAF40B4A1E74A815`
	`/P4_HSB/osv/wahl/leer;jsessionid=A6C209DCB5A1FE198459FF402F586602`
	`/P4_HSB/osv/wahl/navi_unten;jsessionid=09CEC0DADFEA1FF7CAF40B4A1E74A815`
	`/P4_HSB/osv/wahl/navigation;jsessionid=09CEC0DADFEA1FF7CAF40B4A1E74A815`
	`/P4_HSB/osv;jsessionid=09CEC0DADFEA1FF7CAF40B4A1E74A815`
	`/P4_PSB/osv/wahl/Info;jsessionid=86C1CC1D5463438095106A6CDADB74D0`
	`/P4_PSB/osv/wahl/adm_anwender_change_pw_First;jsessionid=A8E9913F60BF7ACDC5D4F1426FC00454`
	`/P4_PSB/osv/wahl/arbeit;jsessionid=86C1CC1D5463438095106A6CDADB74D0`
	`/P4_PSB/osv/wahl/leer;jsessionid=86C1CC1D5463438095106A6CDADB74D0`
	`/P4_PSB/osv;jsessionid=30C1EFDBC56D87F19457A8144E2D7A82`
	`/P5/osv/wahl/adm_anwender_change_pw_First;jsessionid=8A5DBCF421074C69C0C654FE1BB87E9C`
	`[..]`

Description :	Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. An end-user can use OSV and afterwards log out. The next user that takes seat on the same computer and browser can use the back button of the browser to view pages that have previously been viewed by the logged-in user that was logged of. This is because the browser stores all web pages that are viewed, because OSV has not set the HTML cache headers to private.
Impact :	If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.

Recommendation :	The application should return caching directives, instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content:
	
	`Cache-control: no-store`
	`Pragma: no-cache`

Reproduction :	GET /P4_PSB/osv/wahl/befehl;jsessionid=86C1CC1D5463438095106A6CDADB74D0?work=138&level=9&view=0&stepId=1519349128854&HMAC=9q4iyqf0d77ish4bwjfhkbn23 HTTP/1.1 Host: osv.local:8443
Evidence :	HTTP/1.1 200 OK Server: Apache-Coyote/1.1 X-Powered-By: Servlet 2.4; JBoss-4.2.3.GA (build: SVNTag=JBoss_4_2_3_GA date=200807181439)/JBossWeb-2.0 Last-Modified: Thu, 01 Jan 1970 00:00:00 GMT Expires: Fri, 23 Feb 2018 01:26:30 GMT Content-Type: text/html;charset=UTF-8 Vary: Accept-Encoding Date: Fri, 23 Feb 2018 01:25:29 GMT Connection: close [..]
Patch status :	New

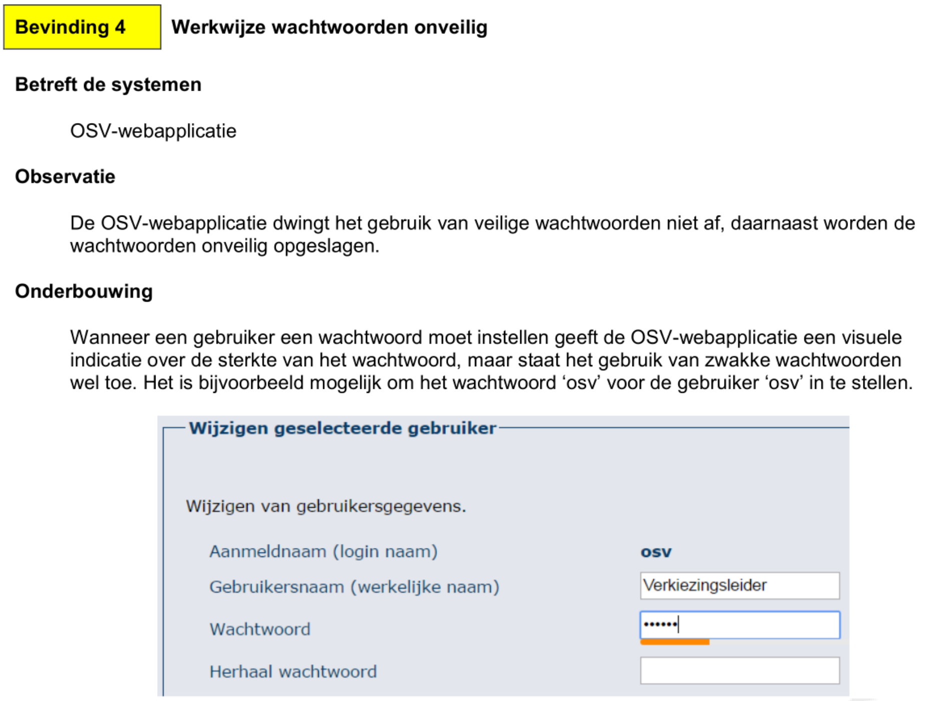
4.1.22 Medium: Password policy not enforced: one letter passwords possible

Risk :	Medium
Hostname :	`osv.local`
Location :	`https://osv.local:8443/P4_PSB/osv/wahl/adm_anwender_change_pw_First`
Description :	The one letter password `a` can be set for user `osv`. The password strength indicator colors red when this password is filled in the initial form for setting the password. This indicator does not enforce its policy, and thus an one letter password could be set.
Impact :	Within a (relatively) short number of attempts, a malicious person could find out the login details of a user account if there are weak passwords in circulation.
Recommendation :	• Change all the identified weak passwords. • Implement a good password policy whereby at a minimum the password length is at least eight characters. Enforce the usage of special characters and numbers.

Reproduction :	`POST`
	`/P4_PSB/osv/wahl/adm_anwender_change_pw_First;jsessionid=86C1CC1D5463`
	`438095106A6CDADB74D0?view=0&level=9&work=110&cmd=adm_change_pw&stepId`
	`=1519348979905&HMAC=4llnc4yji7fk3c6nlt8kg30qv HTTP/1.1`
	`Host: osv.local:8443`
	`Content-Type: application/x-www-form-urlencoded`
	
	`pre_anw_new_pw_1=a&pre_anw_new_pw_2=a&x=8&y=16`

Evidence :	`[..] Wijzigen wachtwoord succesvol afgerond [..]`
Patch status :	Open (not solved)

The Fox IT report states:



Bevinding 4 **Werkwijze wachtwoorden onveilig**

Betreft de systemen

OSV-webapplicatie

Observatie

De OSV-webapplicatie dwingt het gebruik van veilige wachtwoorden niet af, daarnaast worden de wachtwoorden onveilig opgeslagen.

Onderbouwing

Wanneer een gebruiker een wachtwoord moet instellen geeft de OSV-webapplicatie een visuele indicatie over de sterkte van het wachtwoord, maar staat het gebruik van zwakke wachtwoorden wel toe. Het is bijvoorbeeld mogelijk om het wachtwoord 'osv' voor de gebruiker 'osv' in te stellen.

Wijzigen geselecteerde gebruiker

Wijzigen van gebruikersgegevens.

Aanmeldnaam (login naam)	**osv**
Gebruikersnaam (werkelijke naam)	Verkiezingsleider
Wachtwoord	••••••
Herhaal wachtwoord	

4.1.23 Medium: OSV can be run on an unencrypted HTTP connection on port 8080

The Fox IT report states:

- *"[..] De webapplicatie wordt volgens de richtlijnen in verschillende omgevingen gebruikt, waaronder:*

  1. *"Stand-alone" systeem (zonder netwerkverbindingen)*
  2. *Centrale server met meerdere clients ("afgeschermd" netwerk)*

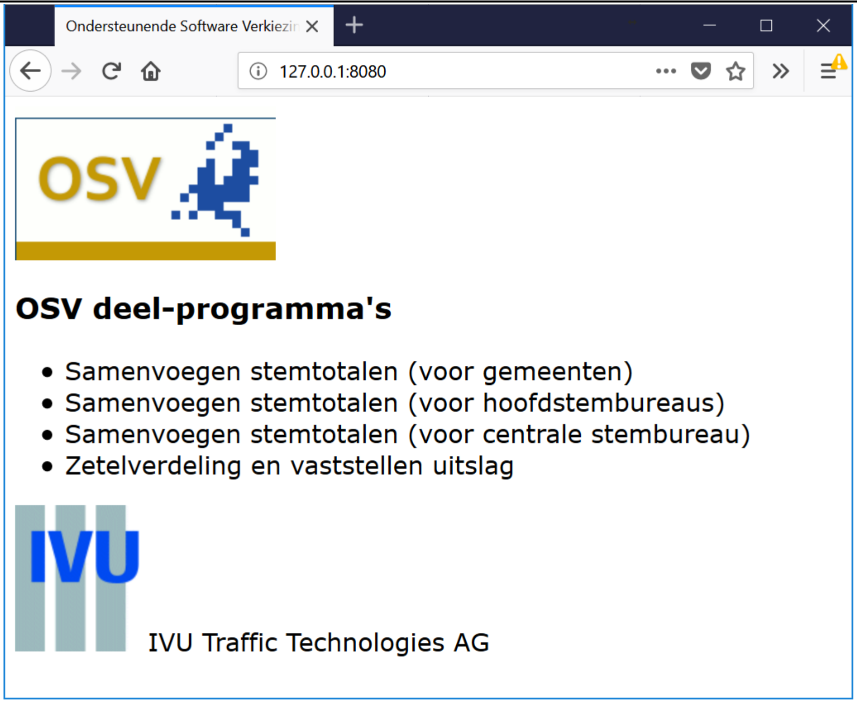
  Wanneer de webapplicatie op een "stand alone" systeem zonder netwerkverbinding wordt gebruikt, dan bevindt het servercomponent en het clientcomponent zich op een en hetzelfde systeem. Een aanvaller die de onversleutelde verbinding wil aanvallen moet zich dus toegang tot dit system verschaffen. Hierdoor heeft de aanvaller dus tevens toegang tot de gegevens van de server en heeft een aanval op het netwerkverkeer weinig meerwaarde.

  Wanneer de webapplicatie in een geïsoleerd netwerk wordt gebruikt met een central servercomponent en meerdere clients dan dient een aanvaller eerst toegang te verkrijgen tot het geïsoleerde netwerk. Indien eenmaal toegang is verkregen tot dit geïsoleerde netwerk dan kan door middel van bijvoorbeeld een man-in-the-middle aanval de onversleutelde verbinding ingezien of gemodificeerd worden.

  Risico
  Afhankelijk van de omgeving waarbinnen OSV gebruikt wordt zal de kans dat een aanvaller de verbinding aanvalt, variëren van laag (geïsoleerd systeem of geïsoleerd netwerk) tot gemiddeld (Mochten de richtlijnen ten aanzien van de infrastructuur niet zijn opgevolgd en wordt toch gebruik gemaakt van gedeelde IT-infrastructuur). De mogelijke gevolgen bij een stand-alone netwerk zijn laag.

  De gevolgen bij gebruik van een netwerk (al dan niet geïsoleerd) zijn hoog. Indien een aanvaller in staat is toegang te verkrijgen tot de onversleutelde verbinding dan is het mogelijk om alle gegevens in te zien alsook te wijzigen. [..]"

Risk :	Medium
Hostname :	`osv.local`
Location :	`http://osv.local:8080/`
Description :	The OSV server can be started to run on port `8080` (HTTP) if the system administrator fails to properly install OSV on port `8443` (HTTPS). On port `8080` an unencrypted connection to OSV is available and can be used. In the OSV manual system administrators are advised to implement encrypted network connections via HTTPS. But when they fail to implement HTTPS, then they may use unencrypted HTTP network connections. This doesn't sound ambitious and is insecure practice.
Impact :	Voting data, usernames and passwords are transmitted over an unencrypted and insecure channel. Also, if OSV is available properly on HTTPS on port used on the same computer and Windows user account with multiple people, a malicious user could leave the OSV login page on port 8080 in the browser. The next person that will use the computer will probably not see that OSV is opened op port `8080`. If the malicious user also leaves a network implant that captures the

	network traffic, then he'll be in the possession of the username and password of each user that logs into OSV on that computer after him/her. Other attack scenario's when a hacker has access to communication between the OSV client and server: 1. Confidential information such as authentication information (passwords) and personal data may be intercepted. This makes identity theft possible. 2. Visitors to the legitimate service (such as a website) can be sent to an almost identical looking, but malicious (*phishing*) service, without the user noticing. 3. The content of the communication can be modified, allowing for example incorrect information to be displayed.
Recommendation :	Only HTTPS port `8443` should be opened on the server. Never allow unencrypted HTTP connections. Permanently close HTTP port `8080` on the OSV server.
Evidence :	 Ondersteunende Software Verkiezi 127.0.0.1:8080 OSV IVU **OSV deel-programma's** - Samenvoegen stemtotalen (voor gemeenten) - Samenvoegen stemtotalen (voor hoofdstembureaus) - Samenvoegen stemtotalen (voor centrale stembureau) - Zetelverdeling en vaststellen uitslag IVU Traffic Technologies AG In file `handleiding_installer_programma4en5.pdf` the following text is present: - *"[..] Mocht blijken dat het tot stand brengen van de HTTPS-verbinding met de client-computers niet goed kan worden doorgevoerd, dan kan worden uitgeweken naar de onbeveiligde HTTP-verbinding. Hiervoor kan de snelkoppeling gebuikt worden, zie figuur 3.6.b. In eerste instantie is dit niet mogelijk en zal er een foutmelding in beeld komen, zie figuur 3.7. Om dit mogelijk te maken dient het bestand HTTP-toegang-toestaan.bat (te vinden in de OSV-installatie map) te worden uitgevoerd, voor snelkoppeling zie figuur 3.8. Hiermee wordt de HTTP-verbinding toegevoegd aan de OSV-server instellingen. [..]"*
Patch status :	Partially solved
Website :	Wikipedia.org: Transport Layer Security

4.1.24 Medium: Strict Transport Security isn't enabled

When the following HTTP request is sent:

```
GET /P4_PSB/osv/logon?r=-1madox HTTP/1.1
Host: osv.local:8443
```

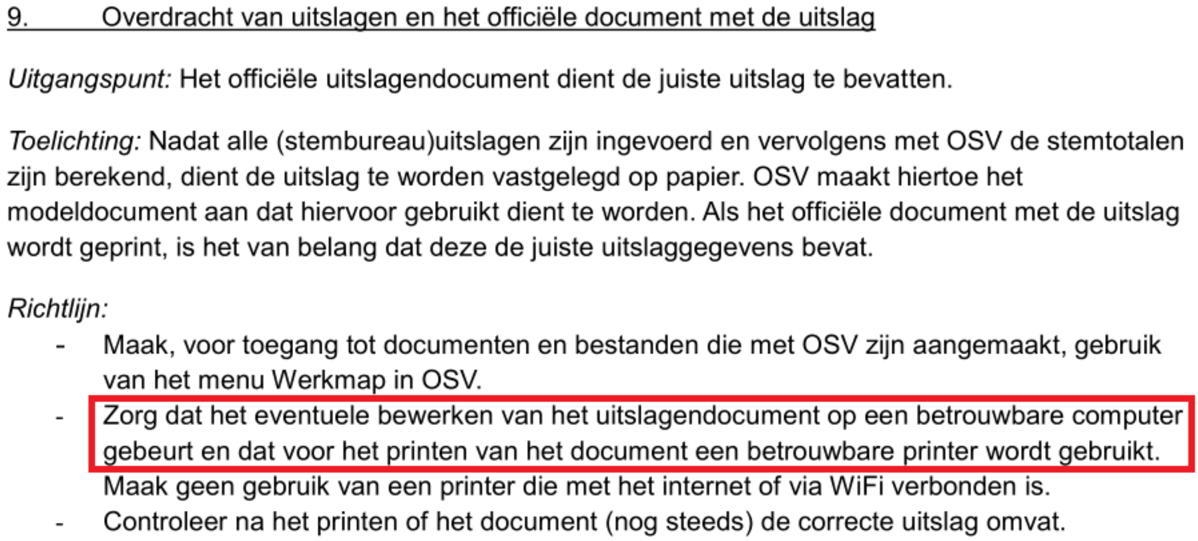
Then the OSV server sends the following HTTP headers:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.4; JBoss-4.2.3.GA (build: SVNTag=JBoss_4_2_3_GA
date=200807181439)/JBossWeb-2.0
Last-Modified: Fri, 23 Feb 2018 02:33:06 GMT
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html;charset=UTF-8
Vary: Accept-Encoding
Date: Fri, 23 Feb 2018 02:33:06 GMT
Connection: close
[..]
```

Risk :	Medium
Description :	The website does not use HTTP Strict Transport Security. Via HTTP Strict Transport Security the browser is configured to only connect via a proper secured HTTPS connection to the website.
Impact :	When a browser uses the HTTP protocol an attacker with access to the traffic between the server and the client can eavesdrop the plain text information that is parsed. As a result, the attacker could access sensitive information like username and password. With Strict Transport Security only HTTPS traffic is allowed to the website by the browser.
Recommendation :	Implement the `Strict-transport-security` HTTP header on all content that is served from the root from a domain name, including on images, etc.
Patch status :	New
Website :	1. Wikipedia: HTTP Strict Transport Security 2. Strict Transport Security draft specification 3. OWASP.org: secure headers project

4.1.25 Medium: Election leader can change election outcome when printing it

When all vote totals are entered into OSV by a municipality, OSV will generate a file that the election leader should download to his computer. The election leader has the possibility to edit the election result in this file on his computer before printing it. There is nowhere mentioned in the OSV instruction below[29] that downloading the election result, printing and validating the printed result should be performed by at least two persons:



9. <u>Overdracht van uitslagen en het officiële document met de uitslag</u>

Uitgangspunt: Het officiële uitslagendocument dient de juiste uitslag te bevatten.

Toelichting: Nadat alle (stembureau)uitslagen zijn ingevoerd en vervolgens met OSV de stemtotalen zijn berekend, dient de uitslag te worden vastgelegd op papier. OSV maakt hiertoe het modeldocument aan dat hiervoor gebruikt dient te worden. Als het officiële document met de uitslag wordt geprint, is het van belang dat deze de juiste uitslaggegevens bevat.

Richtlijn:

- Maak, voor toegang tot documenten en bestanden die met OSV zijn aangemaakt, gebruik van het menu Werkmap in OSV.
- Zorg dat het eventuele bewerken van het uitslagendocument op een betrouwbare computer gebeurt en dat voor het printen van het document een betrouwbare printer wordt gebruikt. Maak geen gebruik van een printer die met het internet of via WiFi verbonden is.
- Controleer na het printen of het document (nog steeds) de correcte uitslag omvat.

Impact

1. The election leader can download and change the election result on his computer before he prints it.
2. The printer could be compromised by a hacker (see also chapter 4.3.1) and change the printed election result. If the printed paper isn't validated, fraud might go unnoticed.

Recommendation

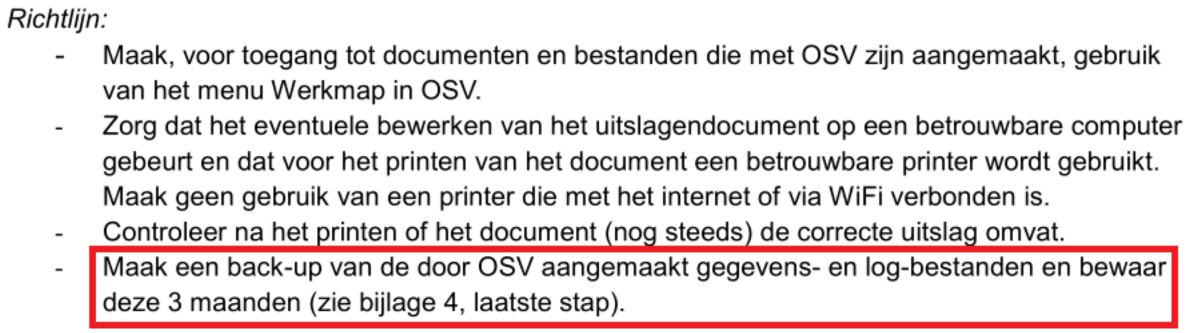
1. Implement a four-eyes procedure for printing the election results.
2. The printer that is used should be part of the offline OSV network. Don't reuse an existing printer from the office network. Buy a new printer that will only be used in elections. Harden the printer properly (latest firmware, password protected, etc.).

Security risk
Medium

[29] See: https://www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/voorwaarden-voor-gebruik-osv

4.1.26 Medium: Lack of transparency of OSV data and log files

The OSV server generates data and log files of all activity on the OSV server. In the OSV security policy[30], system administrators of municipalities are instructed to save these data and log files for 3 months:



Richtlijn:

- Maak, voor toegang tot documenten en bestanden die met OSV zijn aangemaakt, gebruik van het menu Werkmap in OSV.
- Zorg dat het eventuele bewerken van het uitslagendocument op een betrouwbare computer gebeurt en dat voor het printen van het document een betrouwbare printer wordt gebruikt. Maak geen gebruik van een printer die met het internet of via WiFi verbonden is.
- Controleer na het printen of het document (nog steeds) de correcte uitslag omvat.
- Maak een back-up van de door OSV aangemaakt gegevens- en log-bestanden en bewaar deze 3 maanden (zie bijlage 4, laatste stap).

Impact
The log files will not proactive be researched for fraud and anomalies. People that vote have no way to review the data and log files that OSV will generate.

Recommendation
Publish the OSV data and log files in a ZIP file on the website of the municipality, so people can inspect the log files for anomalies.

Security risk
Medium

[30] See: https://www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/voorwaarden-voor-gebruik-osv

4.1.27 Low: No restriction on JavaScript usage via Content Security Policy

When the following HTTP request is sent:

```
GET /P4_PSB/osv/logon?r=-1madox HTTP/1.1
Host: osv.local:8443
```

Then the OSV server sends the following HTTP headers:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.4; JBoss-4.2.3.GA (build: SVNTag=JBoss_4_2_3_GA
date=200807181439)/JBossWeb-2.0
Last-Modified: Fri, 23 Feb 2018 02:33:06 GMT
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html;charset=UTF-8
Vary: Accept-Encoding
Date: Fri, 23 Feb 2018 02:33:06 GMT
Connection: close
[..]
```

Risk :	Low
Description :	The website does not use a Content Security Policy configuration.
Impact :	The usage possibility of JavaScript is not limited by the website. If the website contains a cross-site scripting vulnerability, then JavaScript code can be injected into the web page. This code is then executed by the browser of the victim. If a well-established Content Security Policy is active, the attacker can inject JavaScript code into the browser of the victim, but then the code will not get executed by the browser. A good configured Content Security Policy is a strong protection against cross-site scripting vulnerabilities. **CSP in regarding to the found cross-site scripting** If the `Content-security-policy` HTTP header was used and properly configured, the cross-site scripting vulnerability that was found, would not have manifested. Inline JavaScript code can be prohibited via Content Security Policy and it is advised to do so.
Mitigated :	The lack of a (properly configured) Content Security Policy configuration provides no immediate vulnerability. It is a multi-layered defense against cross-site scripting vulnerabilities.
Recommendation :	1. Enable the Content Security Policy and configure it tight. 2. Make sure that when the content security policy is violated by a browser, that this violation is logged and monitored. Point the content security violation variable `report-uri` to a server-side log script. Implement a process that periodically analyses these logs for programming errors and hack attacks.
Patch status :	New
Website :	1. Wikipedia: Content Security Policy 2. content-security-policy.com 3. An Introduction to Content Security Policy

4.1.28 Low: four-eyes procedure can be deactivated set via the database

An OSV system administrator can change the Derby database (see chapter 4.1.2) and modify OSV to deactivate the four-eyes procedure to circumvent this measure.

The Fox IT report about the four-eyes procedure:

Bevinding 9 **Vier-ogen-principe wordt niet afgedwongen**

Betreft de systemen

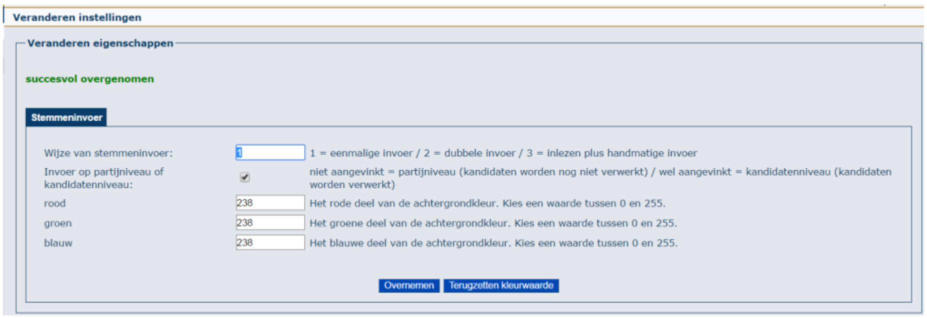
OSV-webapplicatie

Observatie

Het vier-ogen-principe wordt niet volledig afgedwongen door OSV.

Onderbouwing

De OSV-webapplicatie bevat de mogelijkheid om op PSB-, HSB- en CSB-niveau te configureren hoe vaak de stemmeninvoer dient plaats te vinden. Standaard staat de instelling voor PSB op “dubbele invoer”, maar dit kan door de gemeente aangepast worden. Onderstaande afbeelding geeft een succesvolle wijziging van de standaard waarde weer.



Veranderen instellingen

Veranderen eigenschappen

succesvol overgenomen

Stemmeninvoer

Wijze van stemmeninvoer:	1	1 = eenmalige invoer / 2 = dubbele invoer / 3 = inlezen plus handmatige invoer
Invoer op partijniveau of kandidatenniveau:	☑	niet aangevinkt = partijniveau (kandidaten worden nog niet verwerkt) / wel aangevinkt = kandidatenniveau (kandidaten worden verwerkt)
rood	238	Het rode deel van de achtergrondkleur. Kies een waarde tussen 0 en 255.
groen	238	Het groene deel van de achtergrondkleur. Kies een waarde tussen 0 en 255.
blauw	238	Het blauwe deel van de achtergrondkleur. Kies een waarde tussen 0 en 255.

Risico

Indien de invoer niet door middel van het vier-ogen-principe plaatsvindt kunnen al dan niet bewuste invoerfouten optreden bij het invoeren van de stemtotalen op PSB-niveau. Hiermee kunnen mogelijk de resultaten van de verkiezingen beïnvloed worden.

Op HSB-niveau wordt niet afgedwongen dat naast het inlezen van de digitale EML-bestanden tevens de aantallen aan de hand van de papieren processen-verbaal N11 worden ingevoerd. Hierdoor kan een aanvaller die mogelijk het EML-bestand aangepast heeft toch de stemtotalen beïnvloeden en hiermee impact hebben op de verkiezingen.

Op CSB-niveau zijn de gevolgen beperkt vanwege de handmatige telling en berekening, op basis van de papieren processen-verbaal O3, die parallel aan het OSV-proces plaatsvindt.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			
	Gemiddeld		GEMIDDELD	
	Hoog			

Aanbeveling

Fox-IT adviseert om op alle niveaus minimaal het vier-ogen-principe technisch af te dwingen. Hierbij dient de mogelijkheid tot configuratie zoveel mogelijk te worden verwijderd. Tevens wordt aangeraden om op HSB-niveau standaard te kiezen voor de optie waarbij zowel het EML-bestand ingelezen wordt, alsook dat de stemaantallen handmatig ingevoerd dienen te worden.

4.1.29 Low: jQuery security updates are missing

Risk :	Low
Hostname :	`osv.local`

Location :	`https://osv.local:8443/P4_CSB/js/jquery-1.12.4.js`
	`https://osv.local:8443/P4_HSB/js/jquery-1.12.4.js`
	`https://osv.local:8443/P4_PSB/js/jquery-1.12.4.js`
	`https://osv.local:8443/P5/js/jquery-1.12.4.js`
	`https://osv.local:8443/P4_HSB/help/P4/jquery.js`

Description :	jQuery version 1.12.4 is used in P4 and P5. jQuery version 1.11.2 is used in P4. These versions have known security issues. For more information, visit: https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/
Impact :	Patched security vulnerabilities by the software vendor are not implemented in certain JavaScript libraries that are used. This can result in a DOM-based cross-site scripting vulnerability.
Mitigated :	The vulnerability might be affecting a feature of the library that the website is not using. If the vulnerable feature is not used, this alert can be consider as false positive.
Recommendation :	Update jQuery to the latest available version.

Evidence :	`https://osv.local:8443:8443/P4_CSB/js/jquery-1.12.4.js`
	
	`GET /P4_CSB/js/jquery-1.12.4.js HTTP/1.1`
	`Host: osv.local:8443:8443`
	
	`[..] jQuery JavaScript Library v1.12.4 [..]`
	`https://osv.local:8443:8443/P5/js/jquery-1.12.4.js`
	
	`GET /P5/js/jquery-1.12.4.js HTTP/1.1`
	`Host: osv.local:8443:8443`
	
	`[..] jQuery JavaScript Library v1.12.4 [..]`
	`https://osv.local:8443/P4_HSB/help/P4/jquery.js`
	
	`GET /P4_HSB/help/P4/jquery.js HTTP/1.1`
	`Host: osv.local:8443`
	
	`[..] jQuery v1.11.2 | (c) 2005, 2014 jQuery Foundation [..]`

Patch status :	New

4.1.30 Low: OSV is used by default with a non-personal admin account

Risk :	Low
Hostname :	osv.local
Location :	https://osv.local:8443/
Description :	The username of the default administrator non-personal user account in OSV is osv. After logging in with this account for the first time, a new password has to be set. No new username have to be supplied and the username name can't be changed.
Impact :	The audit trail of user osv is harder to trace back to an individual involved system administrator working with the account. When fraud occurs with the user account, it is not directly traceable who did it exactly.
Recommendation :	Let each involved system administrator work under a separate personal OSV user account so the audit trail is more personalized.
Patch status :	Open (not solved)

4.1.31 Low: OSV database software Derby is missing security updates

Risk :	Low
Hostname :	osv.local
Location :	osv.local
Description :	Apache Derby version 10.11.1.1 is used by OSV.
Impact :	Security patches that are already implemented in newer versions of the software are lacking in the used version.
Mitigated :	The Derby database is file-based and does not open an UDP or TCP port on the OSV server. The attack surface to exploit missing Derby security updates is therefor limited.
Recommendation :	Update Derby to the latest version.
Patch status :	New

4.1.32 Low: HTML frames are used

Risk :	Low
Hostname :	osv.local
Location :	https://osv.local:8443/P4_PSB/osv;jsessionid=86C1CC1D5463438095106A6CDADB74D0 https://osv.local:8443/P4_HSB/osv;jsessionid=09CEC0DADFEA1FF7CAF40B4A1E74A815 https://osv.local:8443/P4_HSB/osv/wahl/arbeit;jsessionid=AFD7997042856F951A3135CC5B35C64B?work=39&level=4&view=0&gebietnr=1952&stepId=1519354634487&HMAC=6lc4pc7f7fzbayuvvvvpilhzh https://osv.local:8443/P4_PSB/help/P4/index.html http://osv.local:8080/
Description :	The website uses HTML frames.
Impact :	By using HTML frames, it is not clear to end users what specific URL they are visiting. Users can be redirected to other websites without this being visible to that user.

	Mozilla states the following on the `<frame>` HTML tag: *"[..] This feature has been removed from the Web standards. Though some browsers may still support it, it is in the process of being dropped. Avoid using it and update existing code if possible; see the compatibility table at the bottom of this page to guide your decision. Be aware that this feature may cease to work at any time. [..]"*
Recommendation :	Don't use HTML frames anymore.

Evidence :	`https://osv.local:8443/P4_PSB/osv;jsessionid=86C1CC1D5463438095106A6CDADB74D0`
	
	`GET /P4_PSB/osv;jsessionid=86C1CC1D5463438095106A6CDADB74D0 HTTP/1.1`
	`Host: osv.local:8443`
	
	`[..] <title>plaatselijk stembureau (P4) OSV</title>`
	`[..]`
	`<frameset cols='210,*' border='0' frameborder='no' onload='history.forward()'>`
	`<frameset rows='124,*' border='0' frameborder='no'>`
	`<frame src='/P4_PSB/img/logo/kiesraad.gif' name='Logo' scrolling='no' marginwidth='0' marginheight='0'>`
	`<frame src='/P4_PSB/osv/wahl/leer;=[..]border='0'></frame>`
	`</frameset>`
	`<frameset rows='110,*,0' border='0' frameborder='no'>`
	`<frame src='/P4_PSB/osv/wahl/befehl[..] border='0'></frame>`
	`<frame src='/P4_PSB/osv/wahl/arbeit[..] frameborder='0' framespacing='0' border='0'></frame>`
	`<frame src='/P4_PSB/osv/wahl/refresh;[..]></frame>`
	`</frameset>`
	`</frameset>`
	`[..]`
	
	`https://osv.local:8443/P4_PSB/help/P4/index.html`
	
	`GET /P4_PSB/help/P4/index.html HTTP/1.1`
	`Host: osv.local:8443`
	
	`[..] <title>Handleiding OSV</title>`
	`[..] <iframe name="hmnavigation" id="hmnavigation" src="hmcontent.htm" seamless="seamless" title="Navigation Pane" frameborder="0"></iframe>`
	`[..] document.write('<iframe name="hmcontent" id="hmcontent" src="'+defaulttopic+'" seamless="seamless" title="Content Page" frameborder="0"></iframe>');`
	`[..] <noscript> <iframe name="hmcontent" id="hmcontent" src="overview_aim.htm" seamless="seamless" title="Content Page" frameborder="0"></iframe> </noscript> [..]`

Patch status :	New

4.1.33 Low: Lack of multi-factor authentication on login screen

Risk :	Low
Hostname :	`osv.local`
Location :	`https://osv.local:8443/P4_PSB/jsp/wahl/login_dialog.jsp`
Description :	Only a username and password are required to log into OSV. Two-factor authentication is not supported. There is no check being performed on something a user has physical possession of, such as a smart card, mobile phone or IP address.
Impact :	Passwords are relatively easy to intercept for an attacker and thus fragile: if someone knows the password of someone else, then that person can abuse someone else's identity. This is made more difficult by adding additional controls (factors).
Recommendation :	Implement two-factor authentication for all users, especially for administrator account `osv`.

Reproduction :	`POST`
	`/P4_PSB/jsp/wahl/login_dialog.jsp;jsessionid=BFD09FA2601E0391F321A04FBE6800AA?stepId=1519351993103&HMAC=44ypj0iawkv5chsog7m5p5iue HTTP/1.1`
	`Host: osv.local:8443`
	`Referer: https://osv.local:8443/P4_PSB/osv/logon?r=-y8nwst`
	`Content-Type: application/x-www-form-urlencoded`
	`Content-Length: 67`
	
	`cmd=app_login&User2017=osv&Password2017=qwe&x=15&y=15&cmd=app_login`

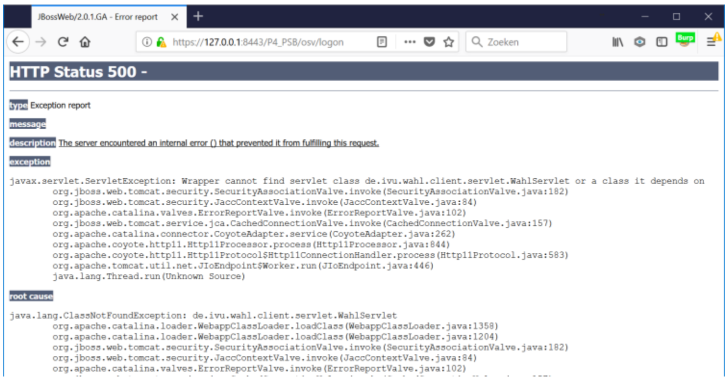
Evidence :	`[..] Gebruiker osv is al aangemeld in het systeem. [..]`
Patch status :	New

4.1.34 Low: JBoss configuration seems not to be hardened

The JBoss configuration of the OSV server sends its version number in the HTTP server's response:

```
GET / HTTP/1.1
Host: osv.local:8443

[..]
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.4; JBoss-4.2.3.GA (build: SVNTag=JBoss_4_2_3_GA
date=200807181439)/JBossWeb-2.0
[..]
```

JBoss also displays technical error messages:


JBossWeb/2.0.1.GA - Error report
https://127.0.0.1:8443/P4_PSB/osv/logon
Zoeken
Burp

HTTP Status 500 -

type Exception report

message

description The server encountered an internal error () that prevented it from fulfilling this request.

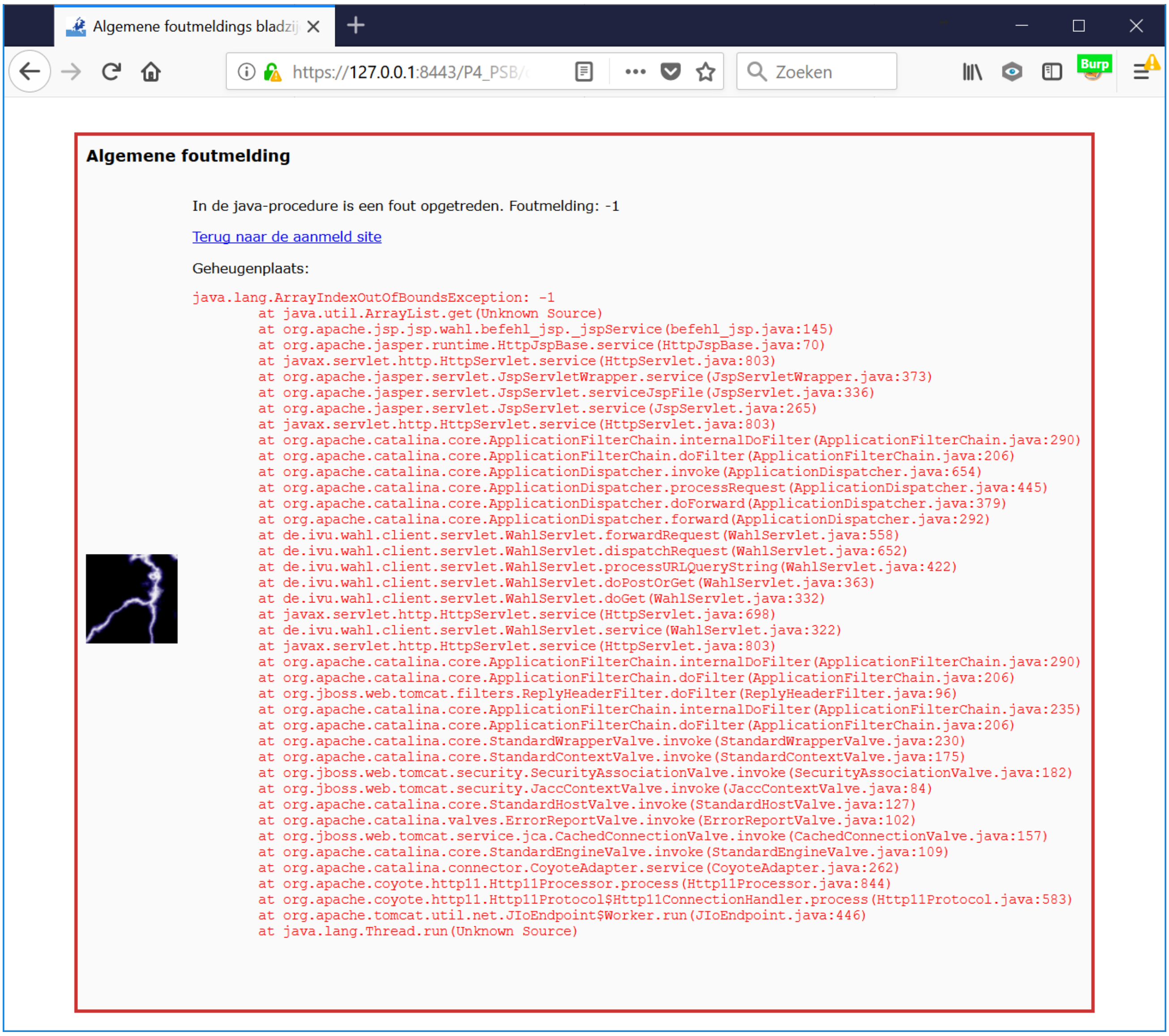
exception

```
javax.servlet.ServletException: Wrapper cannot find servlet class de.ivu.wahl.client.servlet.WahlServlet or a class it depends on
	org.jboss.web.tomcat.security.SecurityAssociationValve.invoke(SecurityAssociationValve.java:182)
	org.jboss.web.tomcat.security.JaccContextValve.invoke(JaccContextValve.java:84)
	org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:102)
	org.jboss.web.tomcat.service.jca.CachedConnectionValve.invoke(CachedConnectionValve.java:157)
	org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:262)
	org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:844)
	org.apache.coyote.http11.Http11Protocol$Http11ConnectionHandler.process(Http11Protocol.java:583)
	org.apache.tomcat.util.net.JIoEndpoint$Worker.run(JIoEndpoint.java:446)
	java.lang.Thread.run(Unknown Source)
```

root cause

```
java.lang.ClassNotFoundException: de.ivu.wahl.client.servlet.WahlServlet
	org.apache.catalina.loader.WebappClassLoader.loadClass(WebappClassLoader.java:1358)
	org.apache.catalina.loader.WebappClassLoader.loadClass(WebappClassLoader.java:1204)
	org.jboss.web.tomcat.security.SecurityAssociationValve.invoke(SecurityAssociationValve.java:182)
	org.jboss.web.tomcat.security.JaccContextValve.invoke(JaccContextValve.java:84)
	org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:102)
```

Java also sends detailed technical debug information including stacktraces when a software error occurs to the browser.



Algemene foutmelding

In de java-procedure is een fout opgetreden. Foutmelding: -1

Terug naar de aanmeld site

Geheugenplaats:

```
java.lang.ArrayIndexOutOfBoundsException: -1
	at java.util.ArrayList.get(Unknown Source)
	at org.apache.jsp.jsp.wahl.befehl_jsp._jspService(befehl_jsp.java:145)
	at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
	at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
	at org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:373)
	at org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:336)
	at org.apache.jasper.servlet.JspServlet.service(JspServlet.java:265)
	at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
	at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
	at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
	at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:654)
	at org.apache.catalina.core.ApplicationDispatcher.processRequest(ApplicationDispatcher.java:445)
	at org.apache.catalina.core.ApplicationDispatcher.doForward(ApplicationDispatcher.java:379)
	at org.apache.catalina.core.ApplicationDispatcher.forward(ApplicationDispatcher.java:292)
	at de.ivu.wahl.client.servlet.WahlServlet.forwardRequest(WahlServlet.java:558)
	at de.ivu.wahl.client.servlet.WahlServlet.dispatchRequest(WahlServlet.java:652)
	at de.ivu.wahl.client.servlet.WahlServlet.processURLQueryString(WahlServlet.java:422)
	at de.ivu.wahl.client.servlet.WahlServlet.doPostOrGet(WahlServlet.java:363)
	at de.ivu.wahl.client.servlet.WahlServlet.doGet(WahlServlet.java:332)
	at javax.servlet.http.HttpServlet.service(HttpServlet.java:698)
	at de.ivu.wahl.client.servlet.WahlServlet.service(WahlServlet.java:322)
	at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
	at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
	at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
	at org.jboss.web.tomcat.filters.ReplyHeaderFilter.doFilter(ReplyHeaderFilter.java:96)
	at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:235)
	at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
	at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:230)
	at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:175)
	at org.jboss.web.tomcat.security.SecurityAssociationValve.invoke(SecurityAssociationValve.java:182)
	at org.jboss.web.tomcat.security.JaccContextValve.invoke(JaccContextValve.java:84)
	at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:127)
	at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:102)
	at org.jboss.web.tomcat.service.jca.CachedConnectionValve.invoke(CachedConnectionValve.java:157)
	at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:109)
	at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:262)
	at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:844)
	at org.apache.coyote.http11.Http11Protocol$Http11ConnectionHandler.process(Http11Protocol.java:583)
	at org.apache.tomcat.util.net.JIoEndpoint$Worker.run(JIoEndpoint.java:446)
	at java.lang.Thread.run(Unknown Source)
```

Impact

As OSV is open source, this is not a real security risk. It is more an indication that the Java configuration was not hardened.

Recommendation

Harden the Java configuration.

Security risk

Low

4.1.35 Low: Checking the integrity of the CD-ROM file is optional

In the The Fox IT report:

- *"[..] **2.3 Transport van cd-roms naar gemeentes***
  De cd-roms met het OSV programma P4 worden door de Kiesraad verstuurd naar alle gemeentes. De gemeentes krijgen instructies om de integriteit van de software op de cd-rom te verifiëren op basis van gepubliceerde cryptografische hashwaardes, alvorens deze te installeren. Hiervoor zijn echter geen maatregelen aanwezig om te waarborgen dat alle gemeentes daadwerkelijk deze integriteitscontrole uitvoeren. Daarnaast maakt de wijze waarop de integriteitscontrole wordt uitgevoerd het mogelijk om deze controle te omzeilen, zoals wordt beschreven in de technische bevindingen.

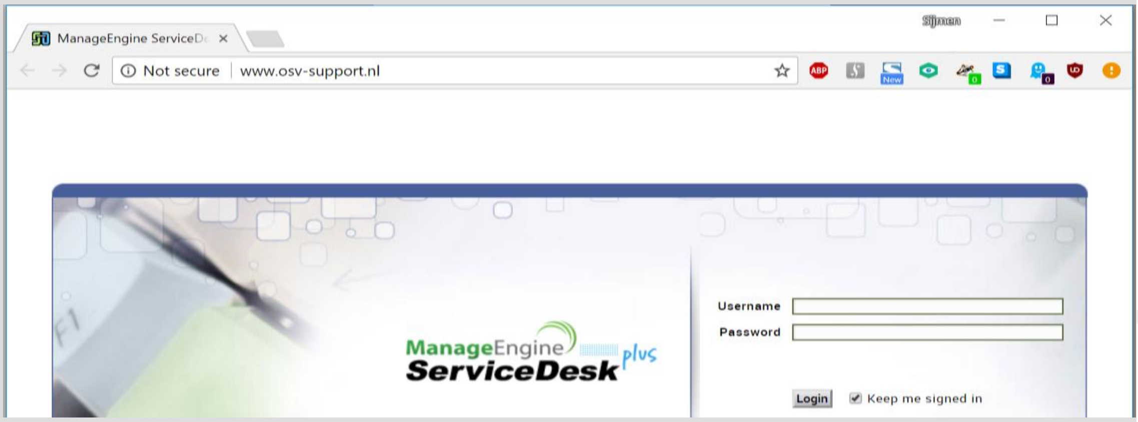
  Als een aanvaller de zending onderschept dan kan deze, afhankelijk van het moment van onderschepping, één of meerdere cd-roms vervangen door aangepaste cd-roms. Naast het onderscheppen van cd-roms tijdens transport kan een aanvaller de gemeentes ook eenvoudigweg een nieuwe cd-rom nasturen en een soortgelijk resultaat bereiken. Een dergelijke aanval is eenvoudiger uit te voeren, maar vereist enige social engineering technieken om de gemeentes zover te krijgen de nieuwe versie over te nemen.

  Afhankelijk van het aantal onderschepte of nagestuurde cd-roms kan de software draaiende bij een of meer gemeentes worden gemanipuleerd. Een dergelijke aanval zou, indien succesvol, ertoe kunnen leiden dat de werking van OSV bij een of meerdere PSB's en/of HSB's gemanipuleerd kan worden. [..]"

Security risk
Low

4.2 In OSV support

4.2.1 High: Passwords transmitted over an unencrypted connection in OSV Support Portal from IVU

Risk :	High
Location :	`http://www.osv-support.nl/`
Description :	OSV users can log into the OSV support portal from IVU. This portal has no encrypted HTTPS connection. The username and password to log into the portal are transmitted over an insecure HTTP connection.
Impact :	When an attacker has access to communication between the client and the server, various attack scenarios are possible: 1. Confidential information such as authentication information (passwords) and personal data may be intercepted. This makes identity theft possible. 2. Visitors to the legitimate service (such as a website) can be sent to an almost identical looking, but malicious (*phishing*) service, without the user noticing. 3. The content of the communication can be modified, allowing for example incorrect information to be displayed.
Recommendation :	1. Implementing Transport Layer Security (TLS). 2. Always set the `Secure` flag for session cookies and other sensitive cookies that should never be sent over unencrypted channels. 3. Implement the `Strict-transport-security` HTTP header on all content that is served from the root from a domain name, including on images, etc. 4. When the website from a usability standpoint is also made available on the HTTP protocol (usually on TCP port 80), then all HTTP traffic should be immediately sent via a permanent 301 redirection to the HTTPS protocol (usually on TCP port 443).
Evidence :	 ManageEngine ServiceD Not secure www.osv-support.nl ManageEngine ServiceDesk plus Username Password Login Keep me signed in
Patch status :	New
Website :	Wikipedia.org: Transport Layer Security

4.2.2 Medium: DNSSEC not enabled

Risk :	Medium
Location :	`osv-support.nl`
Description :	The `DNSSEC` security is not active on the DNS name server.
Impact :	DNS records that the name server sends towards clients are not digitally signed. The integrity of the DNS records that the name server sends towards clients cannot by fully trusted.
Recommendation :	Enable `DNSSEC` on the DNS name server.

Evidence :	`Querying whois.domain-registry.nl for osv-support.nl:`
	
	`Domain name     : osv-support.nl`
	`IP              : 91.212.245.68`
	`Status          : active`
	
	`Registrar:`
	`   1st Gelox GmbH`
	`   Malergasse 16`
	`   93047 REGENSBURG`
	`   Germany`
	
	`Abuse Contact:`
	
	`DNSSEC:       no`
	
	`Domain nameservers:`
	`   ns01.ivu.de`
	`   ns02.ivu.de`
	`   ns03.ivu.de`

Patch status :	New
Website :	SIDN.nl: DNSSEC

4.2.3 Medium: OSV support portal is hosted in Germany

The whois information of domain name osv-supported.nl:

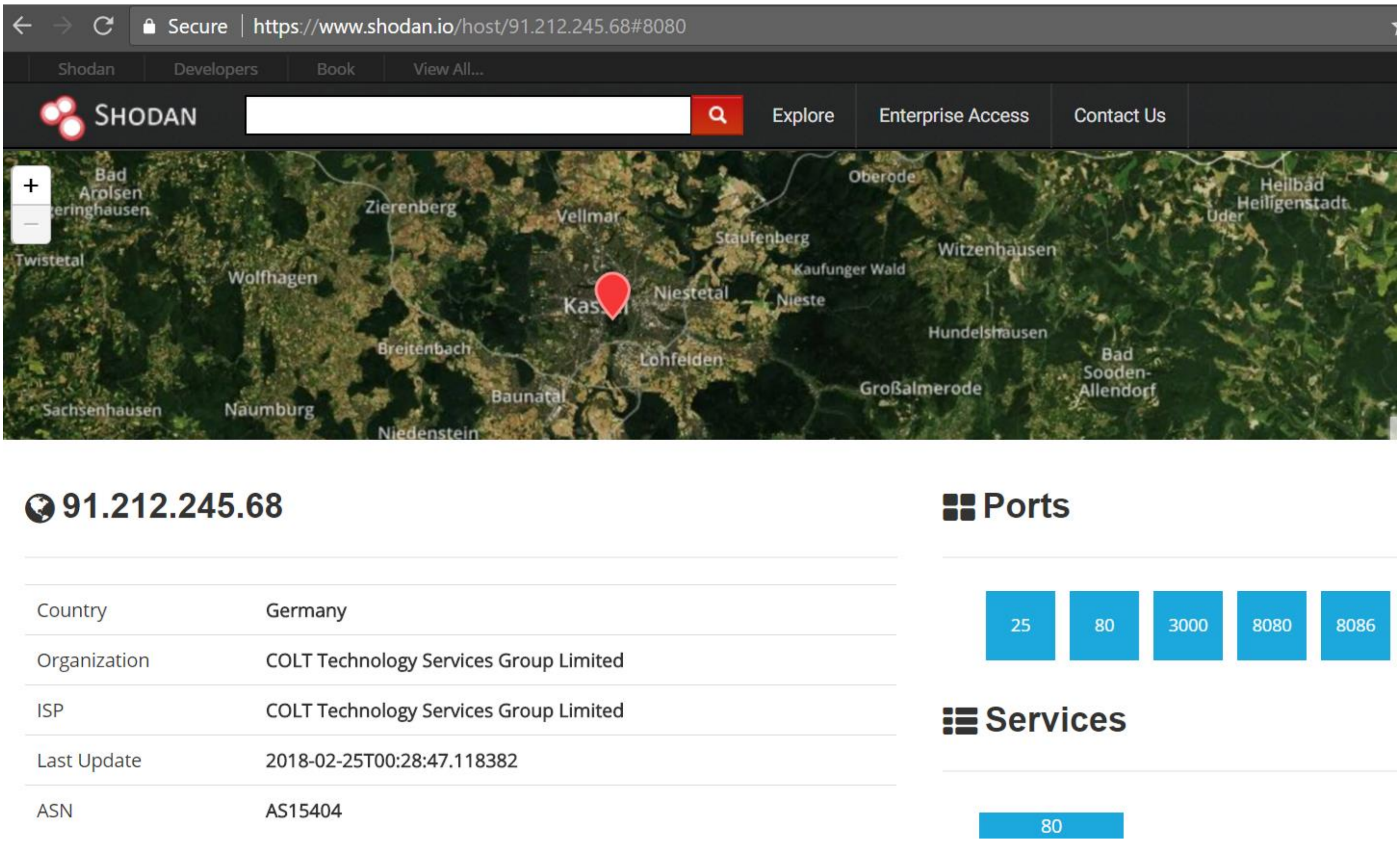
```
Querying whois.domain-registry.nl for osv-support.nl:

Domain name: osv-support.nl
IP:             91.212.245.68
Status:       active

Registrar:
   1st Gelox GmbH
   Malergasse 16
   93047 REGENSBURG
   Germany

Abuse Contact:

<y>DNSSEC:      no</y>
```

```
Domain nameservers:
   ns01.ivu.de
   ns02.ivu.de
   ns03.ivu.de
```

The IP address is registered to IVU-TRAFFIC-TECHNOLOGIES-AG and hosted in Germany:

```
| whois-ip: Record found at whois.ripe.net
| inetnum: 91.212.245.0 - 91.212.245.255
| netname: IVU-TRAFFIC-TECHNOLOGIES-AG
| country: DE
| orgname: IVU Traffic Technologies AG
| organisation: ORG-IVU1-RIPE
| email: post@ivu.de
| person: Michael Degner
|_email: mde@ivu.de
```

Shodan also shows the estimated location of the server in Germany[31]:



91.212.245.68

Country	Germany
Organization	COLT Technology Services Group Limited
ISP	COLT Technology Services Group Limited
Last Update	2018-02-25T00:28:47.118382
ASN	AS15404

Ports

25 80 3000 8080 8086

Services

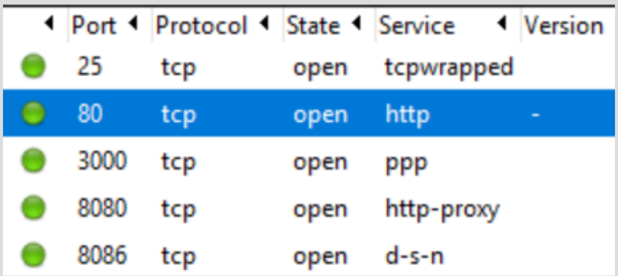
80

Recommendation

The OSV Support Portal www.osv-support.nl should be hosted in The Netherlands.

[31] See: https://www.shodan.io/host/91.212.245.68

4.2.4 Medium: Shodan shows unnecessary ports open on the support portal

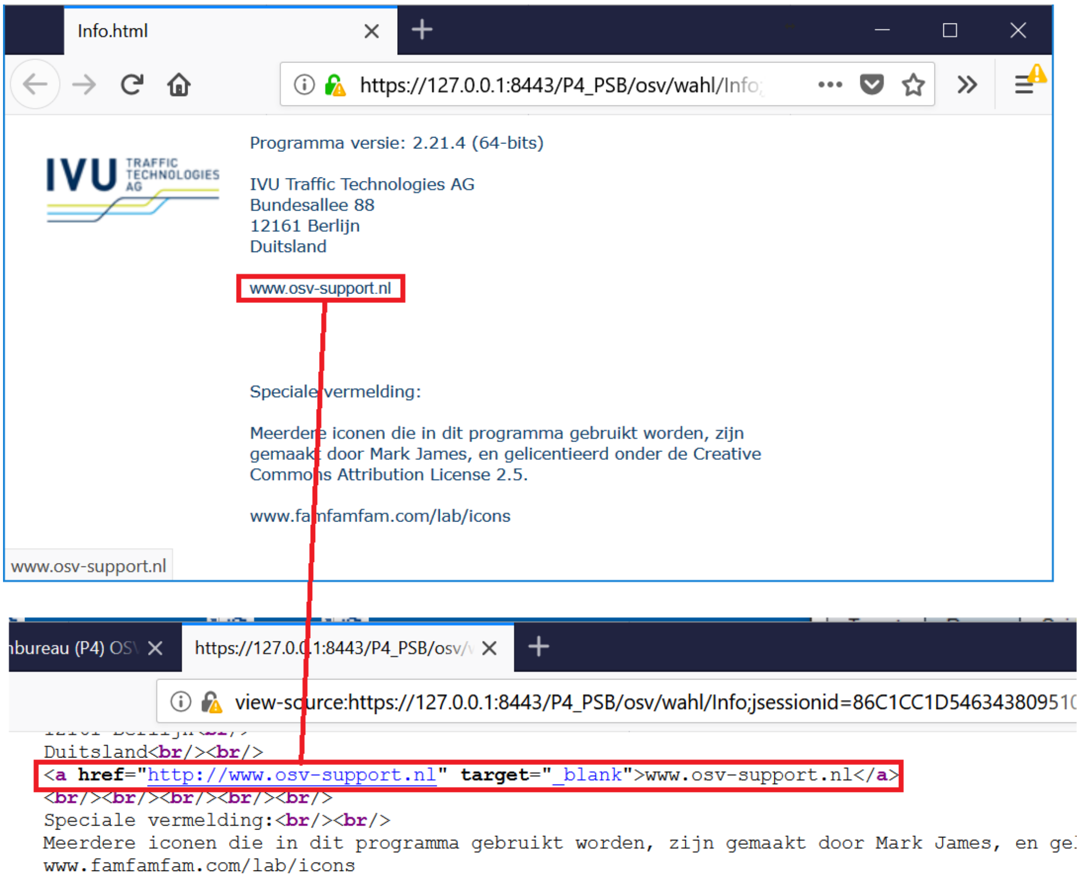
Risk :	Medium
Hostname :	`www.osv-support.nl`
Description :	A port scan showed that unnecessary ports are open on the host.
Impact :	Unnecessary ports widens the attack surface of an attacker, thereby making the host more vulnerable to attacks.
Recommendation :	Make sure that the open ports that are unnecessary for the functioning of the server be shut down.
Evidence:	
Patch status :	New

	Port	Protocol	State	Service	Version
●	25	tcp	open	tcpwrapped	
●	80	tcp	open	http	-
●	3000	tcp	open	ppp	
●	8080	tcp	open	http-proxy	
●	8086	tcp	open	d-s-n	

4.2.5 Very low: Webpage contains insecure links to other websites

Risk :	Very low
Location :	`https://osv.local:8443/P4_PSB/osv/wahl/Info;jsessionid=86C1CC1D5463438095106A6CDADB74D0`
Description :	When logging into OSV, and navigating to the information page, a link is visible to the OSV support portal. But as OSV only should be used on an offline network, it seems odd to included a link to a internet page in OSV. This gives the impression that OSV software developers are not really conscious about the fact that internet is not available (in the past). Also note that an unencrypted HTTP URL is used to navigate to `www.osv-support.nl` instead of an encrypted HTTPS URL. A system administrator could decide to temporary connect the OSV network to the internet initially, to get software-updates for example. The out-going IP address leaks to www.osv-support.nl when an user clicks on the link. The OSV server installation URL also leaks via the `Referer` HTTP header when the user connected to OSV via HTTP port `8080`.
Impact :	1. The system administrator of `www.osv-support.nl` and all the man-in-the-middle parties will see the outgoing IP address of the temporary internet connected OSV network. This external IP address can be used to try to hack into the OSV network. 2. The unsecured HTTP connection to `www.osv-support.nl` can be used to inject malicious JavaScript code by a man-in-the-middle party to try to hack the OSV client browser.
Recommendation :	Remove all links to external websites.

Reproduction :	`GET /P4_PSB/osv/wahl/Info;jsessionid=86C1CC1D5463438095106A6CDADB74D0 HTTP/1.1`
	`Host: osv.local:8443`

Evidence :	
	Info.html
	https://127.0.0.1:8443/P4_PSB/osv/wahl/Info;
	Programma versie: 2.21.4 (64-bits)
	IVU Traffic Technologies AG
	Bundesallee 88
	12161 Berlijn
	Duitsland
	www.osv-support.nl
	Speciale vermelding:
	Meerdere iconen die in dit programma gebruikt worden, zijn gemaakt door Mark James, en gelicentieerd onder de Creative Commons Attribution License 2.5.
	www.famfamfam.com/lab/icons
	www.osv-support.nl
	bureau (P4) OS\
	https://127.0.0.1:8443/P4_PSB/osv/
	view-source:https://127.0.0.1:8443/P4_PSB/osv/wahl/Info;jsessionid=86C1CC1D54634380951(
	`12161 Berlijn<br/>`
	`Duitsland<br/><br/>`
	`<a href="http://www.osv-support.nl" target="_blank">www.osv-support.nl</a>`
	`<br/><br/><br/><br/><br/>`
	`Speciale vermelding:<br/><br/>`
	`Meerdere iconen die in dit programma gebruikt worden, zijn gemaakt door Mark James, en ge`
	`www.famfamfam.com/lab/icons`

Patch status :	New
Website :	1. target="_blank" - the most underestimated vulnerability ever 2. Reverse tabnabbing attacks

4.3 In internal network of municipalities

4.3.1 Medium: BYOD from municipalities could compromise the OSV server

System administrators are allowed to use BYOD USB sticks for transferring files. Most modern laptops, office computers and servers do not have CD-ROM drives anymore. The OSV server that a municipality will deploy will probably not have a CD-ROM drive. It is likely that IT departments of municipalities will open the received CD-ROM on a computer that will not be part of the air-gaped OSV network. This could be an internet connected computer or BYOD every day (office) laptop. The ZIP file on the CD-ROM could then be copied to a BYOD unencrypted USB stick to copy it to the OSV server.

A USB stick is probably used to transfer EML and log files that the OSV server generates to the internal network of a municipality to archive them. These EML files should also be e-mailed to the Electoral Council for inspecting and archiving them.

Fox IT report from 2017 states:

- *"[..] De volgende situaties zouden bijvoorbeeld voor kunnen komen en daarmee kunnen leiden tot afhankelijkheden van de reguliere kantoorautomatisering en daarmee tot reële risico's:*
    - *De OSV-systemen zijn in het verleden gekoppeld aan de reguliere kantoorautomatisering of internet;*
    - *De OSV-systemen en/of –netwerken zijn in strijd met de instructies gekoppeld aan het internet;*
    - *De OSV-systemen en/of netwerken zijn niet verbonden met het internet, maar wel met de kantoorautomatisering;*
    - *De OSV-systemen en/of netwerken zijn "afgeschermd" van alle andere netwerken door middel van een soft- en/of hardwarematige firewall, maar desalniettemin feitelijk verbonden met een kantoorautomatiseringsnetwerk;*
    - *OSV-systemen zijn op netwerk-niveau geïsoleerd, maar gevirtualiseerd op gedeelde hardware en/of het beheer van de virtualisatielaag vindt plaats vanaf (het beheersegment van) de reguliere kantoorautomatisering;*
    - *OSV-systemen worden op enig moment met het internet verbonden om benodigde software van derden, zoals Cygwin, te downloaden;*
    - *Printen van een proces-verbaal vindt plaats buiten de OSV-infrastructuur, bijvoorbeeld vanaf een reguliere werkplek;*
    - *Op de OSV-systemen wordt ongeverifieerde software geïnstalleerd;*
    - *OSV wordt op een reguliere werkplek van cd-rom gekopieerd naar USB-stick om op deze wijze naar de OSV-systemen te transporteren. Dit kan bijvoorbeeld nodig zijn wanneer de OSV-systemen niet beschikken over een cd-rom speler. [..]*

  Daarnaast bestaat de mogelijkheid dat het printen van processen-verbaal plaats kan vinden vanaf een werkplek van de reguliere kantooromgeving van de gemeentes, aangezien daarover geen specifieke instructies worden verstrekt. [..]"

4.4 Electoral Council related

4.4.1 High: Electoral Council doesn't audit municipalities

The Fox IT report from 2017 states:

- *"[..] Er zijn verder geen maatregelen getroffen om te waarborgen en/of controleren dat alle gemeentes daadwerkelijk deze inrichtingsadviezen opvolgen om "stand alone" systemen en/of niet-gekoppelde netwerken te gebruiken. [..]"*

4.4.2 Medium: Electoral Council receives BYOD USB sticks from political parties

Political parties can generate EML files with OSV P1, P2 and P3 that they can sent on BYOD USB sticks to the Electoral Council.

4.4.3 Medium: Security risks of the laptop used by Electoral Council to run OSV on

The Fox IT report from 2017 states:

- *"[..] **3.1.3 Kiesraad (CSB)***
  Bij de Kiesraad (CSB) wordt gebruik gemaakt van een speciaal voor OSV ingerichte laptop. Deze laptop wordt niet voor andere doeleinden gebruikt en wordt fysiek bewaard in een kluis als deze niet in gebruik is. Het P22 proces-verbaal (en de benoemingsbrieven), die worden gegenereerd door middel van deze laptop, worden geprint op een werkplek van de reguliere kantooromgeving van de Kiesraad en vervolgens gecontroleerd (zie ook de navolgende paragraaf "Ministerie van Binnenlandse Zaken").

  Time-boxed technisch onderzoek naar de laptop die het CSB gebruikt voor OSV leidt tot diverse aandachtspunten die in potentie tot het compromitteren van het systeem op enig moment zouden kunnen leiden. De volgende observaties ondersteunen deze conclusie in algemene zin:

  - *Het systeem maakt gebruik van een vooraf geïnstalleerd besturingssysteem en vooraf geïnstalleerde programmatuur die niet strikt noodzakelijk is voor de werking van OSV;*
  - *Het systeem wordt ten behoeve van het updaten van het besturingssysteem, het installeren van vereiste software alsook het proces omtrent de kandidaatstelling en bijbehorende lijsten enkele malen met het internet verbonden. Tijdens het gebruik van de OSV-programma's P4 en P5 wordt het systeem niet meer met het internet verbonden, maar het zou dan al gecompromitteerd kunnen zijn;*
  - *Tijdens de installatie van het systeem worden slechts beperkt maatregelen getroffen om het system verder te beveiligen conform beveiligingsrichtlijnen, zogenaamde 'hardening'. [..]"*

It is unknown if the laptop has been properly secured by the Electoral Council.

4.4.4 Remark: Electoral Council doesn't take any responsibility for OSV

The Kiesraad does not take any responsibility for OSV and does not make any guarantees that it will work properly.

When installing OSV, the system administrator has to accept the following agreement:

- *“De programmatuur en handleidingen (hierna: "Software") zijn bedoeld om gemeenten en politieke partijen te ondersteunen bij de kandidaatstelling en vaststelling van de uitslag van verkiezingen die gehouden worden op grond van de Kieswet. De Software is alleen bedoeld voor de verkiezing waarvoor de cd-rom is uitgeleverd. Deze verkiezing staat vermeld op de voorkant van de cd-rom. De Software is ook beschikbaar voor belangstellenden die de werking van de software willen bestuderen.*
- *Politieke partijen, gemeenten en belangstellenden worden hierna gezamenlijk aangeduid als "Gebruiker".*
- *De Kiesraad kan niet garanderen dat de Software steeds functioneert of vrij is van fouten. De Kiesraad aanvaardt geen aansprakelijkheid voor het functioneren of gebruik van de Software.*
- *Indien de Gebruiker de Software gebruikt voor het aanmaken van een proces-verbaal en/of andere documenten, is de Gebruiker zelf verantwoordelijk voor het controleren van de juistheid en volledigheid daarvan.*
- *Indien de Gebruiker constateert dat de Software onjuistheden bevat, wordt hij verzocht de Kiesraad per omgaande op de hoogte te stellen via kiesraad@kiesraad.nl.*
- *De Kiesraad verleent hierbij aan de Gebruiker het kosteloze, herroepelijke en niet-exclusieve recht tot het gebruik van de Software. Het gebruiksrecht eindigt van rechtswege twee maanden na de vaststelling van de uitslag van de desbetreffende verkiezing.*
- *De Gebruiker mag de Software uitsluitend gebruiken (i) ten behoeve van de verkiezing waarvoor de cd-rom is uitgeleverd. Deze verkiezing staat vermeld op de voorkant van de cd-rom of (ii) teneinde de werking daarvan te bestuderen. De Software mag door de Gebruiker uitsluitend worden gebruikt voor zichzelf of zijn eigen organisatie.*
- *Het gebruiksrecht is niet overdraagbaar. Het is de Gebruiker niet toegestaan de Software en dragers waarop deze is vastgelegd te verkopen, te verhuren, te sublicentiëren, te vervreemden of daarop beperkte rechten te verlenen of op welke wijze of voor welk doel dan ook ter beschikking van een derde te stellen.*
- *De Gebruiker is zelf verantwoordelijk voor de installatie van de Software op de benodigde computerapparatuur.*

> *Alle intellectuele eigendomsrechten op de Software en alle daarbij behorende materialen, berusten bij de Kiesraad. Het is de gebruiker niet toegestaan enige aanduiding omtrent auteursrechten of andere rechten van intellectuele eigendom uit de Software en alle daarbij behorende materialen te verwijderen of te wijzigen.”*

It is very remarkable that Electoral Council does not take any responsibility in the terms of agreement that OSV will function properly. This does not sound very trustworthy and responsible.

According to the terms of agreement the municipality that uses OSV is responsible to validate if OSV is working properly. How to do that exactly is nowhere mentioned in the documentation shipped with OSV.

4.4.5 Remark: Restricted distribution of OSV P4 & P5 software: only if you ask for it

The compiled OSV P4 and P5 software (308 MB) that municipalities will install on their local OSV network is not published on www.kiesraad.nl. It is only sent by post if your explicitly ask the Electoral Council for it. Only the Java OSV source code (4,16 MB) is published on the website of the Kiesraad.[32]

Impact

1. The closed OSV P4 and P5 software distribution makes the code not widely available for inspection. Curious independent security researchers will not take the hurdle and time to ask Electoral Council permission to send them the OSV software by post. The Electoral Council stated to RTL News that they were the first party to ask for the CD-ROM file for inspecting OSV.
2. Researcher could look for weaknesses in the Java source code that is published on the website of the Kiesraad, but it is impossible to tell if this source code (4,16 MB) is the same software (308 MB) that municipalities will run on their computers.

Recommendation
Publish the contents on www.kiesraad.nl of the CD-ROM with OSV P4 and P5 on it that is sent to municipalities.

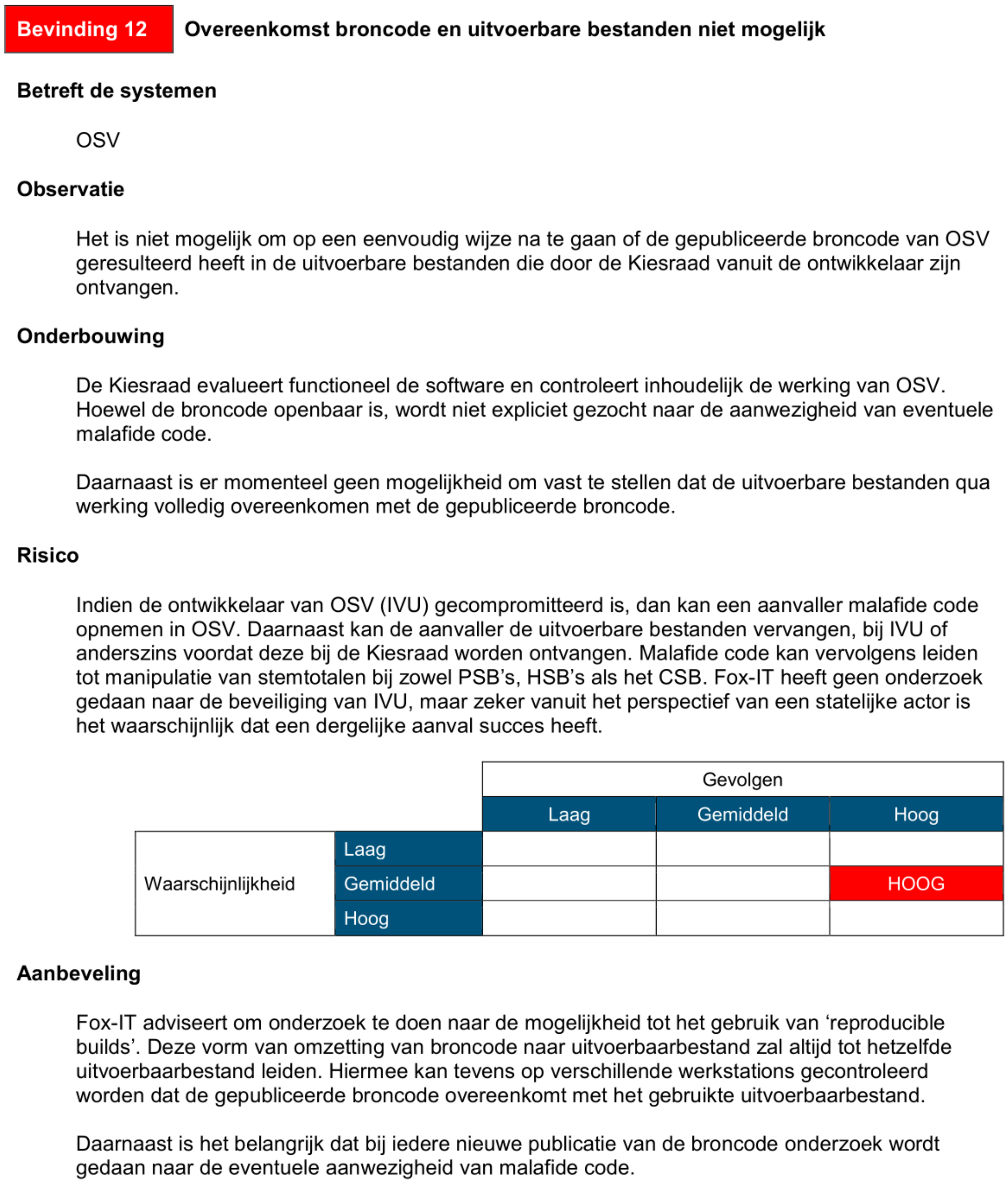
[32] See: https://www.kiesraad.nl/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/osv-broncode-programma-4-en-5-versie-2.21.4

4.5 IVU related

4.5.1 High: OSV might get compromised via IVU

The Fox IT report from 2017 states:

- *"[..] Ongeacht de instantie die de software ter ondersteuning van het stemtelproces ontwikkelt, bestaat de kans dat deze instantie op enigerlei wijze gecompromitteerd wordt. Fox-IT heeft geen onderzoek gedaan naar de beveiliging van de systemen en/of processen van de huidige ontwikkelaar IVU. Indien bijvoorbeeld de ontwikkelsystemen aan het internet gekoppeld zijn, dan kan niet anders geconcludeerd worden dan dat de mogelijkheid tot het compromitteren van de softwareontwikkelaar aanwezig is. In een dergelijk geval zou OSV aangepast kunnen worden voordat deze aan alle andere organisaties in de keten wordt verstrekt. [..]"*



Bevinding 12 **Overeenkomst broncode en uitvoerbare bestanden niet mogelijk**

Betreft de systemen

OSV

Observatie

Het is niet mogelijk om op een eenvoudig wijze na te gaan of de gepubliceerde broncode van OSV geresulteerd heeft in de uitvoerbare bestanden die door de Kiesraad vanuit de ontwikkelaar zijn ontvangen.

Onderbouwing

De Kiesraad evalueert functioneel de software en controleert inhoudelijk de werking van OSV. Hoewel de broncode openbaar is, wordt niet expliciet gezocht naar de aanwezigheid van eventuele malafide code.

Daarnaast is er momenteel geen mogelijkheid om vast te stellen dat de uitvoerbare bestanden qua werking volledig overeenkomen met de gepubliceerde broncode.

Risico

Indien de ontwikkelaar van OSV (IVU) gecompromitteerd is, dan kan een aanvaller malafide code opnemen in OSV. Daarnaast kan de aanvaller de uitvoerbare bestanden vervangen, bij IVU of anderszins voordat deze bij de Kiesraad worden ontvangen. Malafide code kan vervolgens leiden tot manipulatie van stemtotalen bij zowel PSB's, HSB's als het CSB. Fox-IT heeft geen onderzoek gedaan naar de beveiliging van IVU, maar zeker vanuit het perspectief van een statelijke actor is het waarschijnlijk dat een dergelijke aanval succes heeft.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			
	Gemiddeld			HOOG
	Hoog			

Aanbeveling

Fox-IT adviseert om onderzoek te doen naar de mogelijkheid tot het gebruik van 'reproducible builds'. Deze vorm van omzetting van broncode naar uitvoerbaarbestand zal altijd tot hetzelfde uitvoerbaarbestand leiden. Hiermee kan tevens op verschillende werkstations gecontroleerd worden dat de gepubliceerde broncode overeenkomt met het gebruikte uitvoerbaarbestand.

Daarnaast is het belangrijk dat bij iedere nieuwe publicatie van de broncode onderzoek wordt gedaan naar de eventuele aanwezigheid van malafide code.

4.5.2 Very low: Publication of e-mail addresses

Risk :	Very low
Hostname :	`osv.local`
Location :	`https://www.kiesraad.nl/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/osv-broncode-programma-4-en-5-versie-2.21.4`

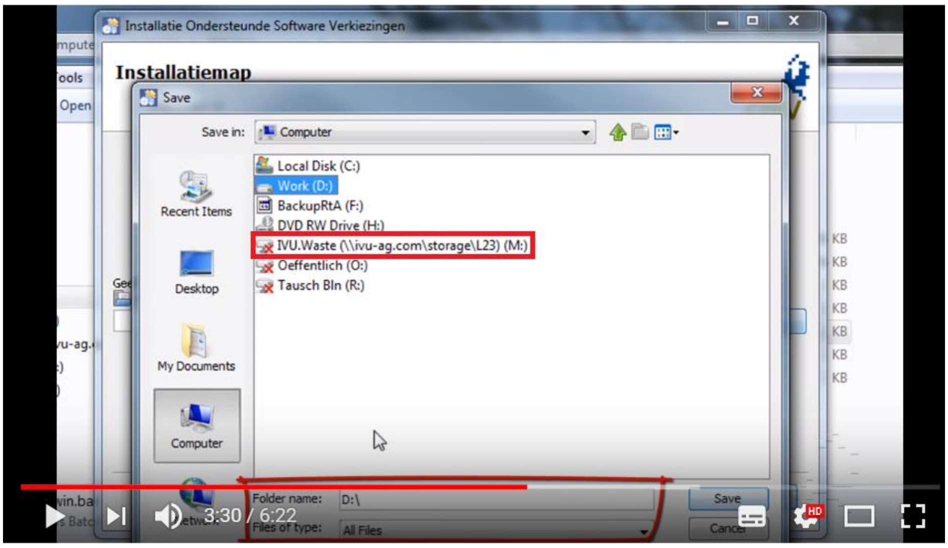
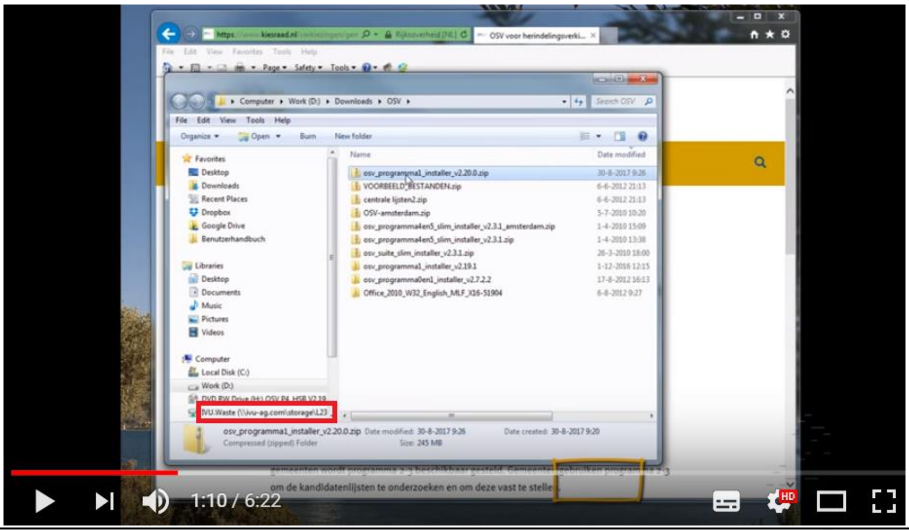
Description :	11 e-mail addresses of OSV developers were found in the Java source code, sorted by times of occurrence:
	
	`cos@ivu.de = 364, core developer, Dr. Domagoj Cosic`
	`jon@ivu.de = 145, core developer`
	`mur@ivu.de = 65`
	`ugo@ivu.de = 38`
	`klie@ivu.de = 25`
	`tdu@ivu.de = 23`
	`bae@ivu.de = 8`
	`sma@ivu.de = 5`
	`mike@ivu.de = 5`
	`tst@ivu.de = 5`
	`apa@ivu.de = 2`

Impact :	E-mail addresses can be used for targeted spear phishing attacks.
Recommendation :	Remove the e-mail addresses. Never publish developer e-mail addresses for more operational security.

Evidence :	`https://osv.local:8443/P4_CSB/js/jquery-entropizer.js`
	
	`GET /P4_CSB/js/jquery-entropizer.js HTTP/1.1`
	`Host: osv.local:8443`
	
	`[..]  * Buckets changed by jon@ivu.de [..]`
	
	`https://osv.local:8443/P4_HSB/js/jquery.autocomplete.js`
	
	`GET /P4_HSB/js/jquery.autocomplete.js HTTP/1.1`
	`Host: osv.local:8443`
	
	`[..]  * tdu@ivu.de, IVU Traffic Technologies AG [..]`

Patch status :	New

4.5.3 Very low: Publication of technical information on the internal network

Risk :	Very low
Location :	`https://www.youtube.com/watch?v=30ZTAr0yYkI&feature=youtu.be`
Description :	The location of an internal IVU network share (`\\ivu-ag.com\storage\L23\IVU.Waste`) is visible in a YouTube video. In 2017 YouTube videos were also leaking internal network shares.
Impact :	Technical information about the environment can help an attacker to further launch specific attacks.
Recommendation :	Screen YouTube videos before publication to check if confidential technical information is leaking.
Reproduction :	Visit: `https://www.youtube.com/watch?v=30ZTAr0yYkI&feature=youtu.be`
Evidence :	`/Screenshots/youtube video laadt software van IVU rik ten arve zien`  Installatie Ondersteunde Software Verkiezingen Installatiemap Save Save in: Computer Recent Items Desktop My Documents Computer Local Disk (C:) Work (D:) BackupRtA (F:) DVD RW Drive (H:) IVU.Waste (\\ivu-ag.com\storage\L23) (M:) Oeffentlich (O:) Tausch Bln (R:) Folder name: D:\ Files of type: All Files Save Cancel 3:30 / 6:22  https://www.kiesraad.nl/verkiezingen/gem OSV voor herindelingsverki... Computer ▸ Work (D:) ▸ Downloads ▸ OSV ▸ File Edit View Tools Help Organize Open Burn New folder Favorites Desktop Downloads Recent Places Dropbox Google Drive Benutzerhandbuch Libraries Desktop Documents Music Pictures Videos Computer Local Disk (C:) Work (D:) DVD RW Drive (H:) OSV P4 HSB V2.19 IVU.Waste (\\ivu-ag.com\storage\L23 Name — Date modified osv_programma1_installer_v2.20.0.zip — 30-8-2017 9:26 VOORBEELD_BESTANDEN.zip — 6-6-2012 21:13 centrale lijsten2.zip — 6-6-2012 21:13 OSV-amsterdam.zip — 5-7-2010 10:20 osv_programma4en5_slim_installer_v2.3.1_amsterdam.zip — 1-4-2010 15:09 osv_programma4en5_slim_installer_v2.3.1.zip — 1-4-2010 13:38 osv_suite_slim_installer_v2.3.1.zip — 26-3-2010 18:00 osv_programma1_installer_v2.19.1 — 1-12-2016 12:15 osv_programma0en1_installer_v2.7.2.2 — 17-8-2012 16:13 Office_2010_W32_English_MLF_X16-51904 — 6-8-2012 9:27 osv_programma1_installer_v2.20.0.zip Date modified: 30-8-2017 9:26 Date created: 30-8-2017 9:20 Compressed (zipped) Folder Size: 245 MB gemeenten wordt programma 2-3 beschikbaar gesteld. Gemeenten gebruiken programma 2-3 om de kandidatenlijsten te onderzoeken en om deze vast te stelle
Patch status :	Reopend

4.5.4 Remark: Dutch election software is made by a German company

The OSV software that is used in Dutch elections is made by a German software company (IVU).

Impact
Germany (secret service) could - if they want to do it - to influence Dutch elections by secretly introducing backdoors in OSV and manipulate OSV output by forcing IVU to cooperate.

Looking at the current political climate, it is highly unlikely that Germany would do so. But it should be marked that Germany is the only country that invaded The Netherlands (for 5 years) in the last 100 years.

Recommendation
Software that is used in Dutch elections should at least be made by Dutch citizens.

4.5.5 Remark: Some municipalities do not seem to have an OSV service contract with IVU

The Electoral Council states on their website[33] an interesting remark about OSV support:

- *"[..] De helpdesk van IVU is bereikbaar op nummer 0318-765000 (voor gemeenten die een servicecontract hebben afgesloten met IVU). [..]"*

Reading this sentence, it gives the impression that there are municipalities that do not have a service contract with OSV vendor IVU.

4.5.6 Remark: OSV instruction meetings are optional for IT departments of municipalities

The Electoral Council states on their website[34]:

- *"[..] **Instructiebijeenkomst***
  Op verschillende locaties organiseert IVU instructiebijeenkomsten voor gemeenten. Tijdens deze bijeenkomsten wordt ingegaan op het gebruik van de OSV programma's 4 en 5 voor de vaststelling van de uitslag. Aanmelden voor een van de bijeenkomsten kan door middel van het aanmeldingsformulier onder aan deze pagina. In het aanmeldformulier staan de locaties en data van de bijeenkomsten. U moet het aanmeldingsformulier ingevuld opsturen naar osv@ivu.nl. [..]"

[33] See: https://www.kiesraad.nl/verkiezingen/gemeenteraden/ondersteunende-software-verkiezingen-osv/osv-voor-gemeenten

[34] See: https://www.kiesraad.nl/verkiezingen/gemeenteraden/ondersteunende-software-verkiezingen-osv/osv-voor-gemeenten