Softwareversies van gemeentelijke websystemen in kaart gebracht

4 februari 2013

Wouter S. van Dongen MSc CISSP
wouter.vandongen at dongit.nl

Kim Vahl MSc
kim.vahl at dongit.nl

Versie 1.3
http://www.dongit.nl

Inhoudsopgave

1 Inleiding

De Diginotar-crisis en Lektober hebben eind 2011 aangetoond dat de ICT van gemeenten kwetsbaar is. Deze kwetsbaarheden bleken vaak voort te komen uit het feit dat software niet of niet tijdig werd geüpdate. Zo bleek bijvoorbeeld dat de website van Diginotar gebruik maakte van een verouderd content management system dat ruim twee jaar niet was geüpdate[1] en dat 50 gemeentelijke systemen draaiden op een verouderde, kwetsbare Windows versie[2]. In 2012 zijn veel maatregelen genomen om herhaling te voorkomen. Bijvoorbeeld verplichte audits en pentesten voor DigiD-afnemers, duidelijke webapplicatiebeveiligingsrichtlijnen van het Nationaal Cyber Security Centrum en de gemeentelijke Informatiebeveiligingsdienst (IBD) van de VNG en KING die moet toezien op de veiligheid van gegevens bij lokale overheden.

Dit onderzoek toont de resultaten van een versieonderzoek van webapplicaties en onderliggende software zoals webservers en database management systems bij alle gemeenten. Hierbij is getracht alle webapplicaties en technieken in kaart te brengen en de versie te achterhalen, waardoor te zien is of de versie up-to-date is. De scope van dit onderzoek betreft alle webapplicaties en services met een (sub)domein van een Nederlandse gemeente. Er is getracht om ook verborgen systemen te detecteren die vaak over het hoofd gezien of vergeten worden, zoals testsystemen. De data voor dit onderzoek is verzameld rond 24 december 2012.

2 Het belang van een solide updatemechanisme

Het up-to-date houden van software is een essentieel onderdeel van ICT-beveiliging. Daarom classificeert het Nationaal Cyber Security Centrum het hebben van een solide updatemechanisme in de "ICT-beveiligingsrichtlijnen voor webapplicaties"[3] als 'hoog'. Dagelijks verschijnen op internet beveiligingsadviezen van verschillende leveranciers waarin de leverancier een kwetsbaarheid in één van zijn softwareproducten beschrijft. Het is belangrijk geleverde updates snel te installeren om de kwetsbaarheid te verhelpen. De eerste stap die hackers daarom vaak ondernemen is het in kaart brengen van de applicaties en services. Welke technieken worden gebruikt en welke softwareversies worden gebruikt? Vervolgens kan op internet eenvoudig gezocht worden naar aanwezige kwetsbaarheden en kan in sommige gevallen kant-en-klare code gevonden worden om de kwetsbaarheid te misbruiken. De meeste ICT-beheerders zijn zich hier gelukkig van bewust en voeren, zoals het hoort, updates uit. Echter vindt het uitvoeren van updates vaak niet snel genoeg plaats waardoor systemen soms weken of maanden kwetsbaar blijven. Soms wordt niet geüpdate omdat functionaliteiten na de update niet meer naar

[1] Zie http://www.nu.nl/internet/2961331/zwaar-verouderde-website-was-oorzaak-diginotar-hack.html

[2] Zie http://webwereld.nl/nieuws/108184/lektober-superknaller--megalek-treft-50-gemeenten.html

[3] Zie https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

behoren werken. Een ander probleem is dat men het overzicht verliest van de gebruikte software waardoor updates niet overal doorgevoerd worden. Tevens worden systemen die minder belangrijk gevonden worden vaak verwaarloosd. Hackers kunnen deze systemen gebruiken om de beter beveiligde systemen aan te vallen.

3 Aannames

De resultaten zijn gebaseerd op software waarvan de versie achterhaald kon worden. Het is niet mogelijk om met absolute zekerheid na te gaan of de softwareversie die gedetecteerd is ook daadwerkelijk die versie is. Hoewel het zeer aannemelijk is dat dit wel zo is, is het mogelijk dat de software banner bijvoorbeeld handmatig door een beheerder gezet is.

Voorts kan het zijn dat kwetsbaarheden in software niet van toepassing zijn op het betreffende systeem. Dit kan bijvoorbeeld komen omdat een patch geïnstalleerd is of package updates, of doordat kwetsbare onderdelen door een bepaalde configuratie uitgeschakeld zijn.

Elk IP-adres wordt in dit onderzoek als een apart systeem beschouwd. In werkelijkheid is het mogelijk dat één systeem meerdere IP-adressen heeft. Verder is het mogelijk dat achter één IP-adres meerdere systemen huizen door technieken als NAT, loadbalancing etc. In dit geval is het voor beheerders van belang dat alle systemen up-to-date gehouden worden.

4 Dataverzamelmethode

Om de benodigde data te verzamelen is een Pythonscript geschreven (Explorer genaamd). Explorer bestaat uit de volgende drie onderdelen:

4.1 Subdomeinverzamelaar

De input van Explorer zijn de hoofddomeinen van gemeenten, bijvoorbeeld 'amsterdam.nl' of 'leiden.nl'. Het verzamelen van subdomeinen geschiedt door middel van drie opeenvolgende methodes:

Als eerste probeert Explorer door middel van een DNS zone transfer alle subdomeinen van een hoofddomein te achterhalen. Hiervoor is als basis DNS Recon gebruikt[4], DNS Recon is aangepast om resultaten in het correcte formaat aan Explorer te overhandigen. Een zone transfer is echter alleen mogelijk wanneer een DNS-server deze functionaliteit niet correct heeft afgeschermd. Indien de zone transfer succesvol heeft plaatsgevonden zijn alle bestaande subdomeinen verzameld en heeft het geen zin om nog meer subdomeinverzameltechnieken toe te passen voor dit domein.

Wanneer een zone transfer niet is geslaagd wordt getracht subdomeinen te bruteforcen. Bruteforcen houdt in dat simpelweg geprobeerd wordt of een subdomein bestaat. De DNS-

[4]Beschikbaar via: https://github.com/darkoperator/dnsrecon

bruteforcefunctionaliteit is tevens ontleend aan DNS Recon. Voor het bruteforcen is een lijst van 1500 woorden gebruikt die gebaseerd op de namelist van DNS Recon. Deze lijst is verder aangevuld met ongeveer 125 veelvoorkomende en/of voor de hand liggende domeinen die bij gemeenten gebruikt worden.

Na uitvoeren van het bruteforceonderdeel worden zoekmachines doorzocht. Hiervoor worden Bing, Google en Google Ajax API gebruikt. Deze drie services leverden vaak verschillende zoekresultaten op. Reeds ontdekte domeinen via het bruteforcen worden als filter ingesteld om zo min mogelijk verzoeken naar de zoekmachines te hoeven sturen.

Van alle verzamelde subdomeinen wordt een DNS-lookup uitgevoerd en worden de IP-adressen en de resultaten door Explorer opgeslagen.

4.2 Poortscan

Op alle verzamelde IP-adressen wordt een poortscan uitgevoerd. Hier is een licht aangepaste versie van python-nmap library gebruikt zodat alle benodigde informatie uit de NMAP-scan aan Explorer wordt geretourneerd. Als eerste wordt een TCP-SYN-scan uitgevoerd om te bepalen welke services op de server beschikbaar zijn, vervolgens wordt getracht de versie van de software te achterhalen. Wanneer de hostname van de server een onbekend subdomein is, slaat Explorer deze op om later te controleren of hier een webapplicatie op actief is.

4.3 HTTP-verzoeken

In dit onderdeel worden HTTP-verzoeken naar alle poorten gestuurd waarop een webserver luistert. Het doel hiervan is om te achterhalen welke technieken gebruikt worden en wat voor webapplicatie het is. Het versturen van verzoeken wordt aan de hand van het voorbeeld hieronder toegelicht.
Verzamelde informatie:

1. Subdomein: cmstest.dongit.nl
2. IP-adres: 95.211.164.65
3. Open poorten: 22 (SSH), 80 (http), 443 (https), 8080 (http-alt), 8443 (https-alt)

Alleen op de http, https, http-alt en https-alt luistert een webserver. Te benaderen URL's op basis van de verzamelde informatie:

1. http://cmstest.dongit.nl
2. https://cmstest.dongit.nl
3. http://cmstest.dongit.nl:8080
4. https://cmstest.dongit.nl:8443

5. http://95.211.164.65
6. https://95.211.164.65
7. http://95.211.164.65:8080
8. https://95.211.164.65:8443

Daarnaast wordt voor elke URL getracht een aantal directories te benaderen. Zo worden bijvoorbeeld om de veel gebruikte webapplicatie phpMyadmin te detecteren de directories 'phpMyAdmin' en 'phpmyadmin' benaderd:

1. http://cmstest.dongit.nl/phpmyadmin/
2. http://cmstest.dongit.nl/phpMyAdmin/
3. https://cmstest.dongit.nl/phpmyadmin/
4. https://cmstest.dongit.nl/phpMyAdmin/
5. etc.

Wanneer de poortscan van een IP-adres niet succesvol is afgerond worden verzoeken verstuurd naar de meest voor de hand liggende poorten 80 (HTTP) en 443 (HTTPS). De poortscan kan bijvoorbeeld door een firewall geblokkeerd worden, door alsnog verzoeken naar poort 80 en 443 te sturen kunnen webapplicaties gedetecteerd worden.

Als eerste wordt met een aanpaste versie van de PHP Wappalyzer driver[5] een verzoek gestuurd om globaal inzichtelijk te maken welke technieken gebruikt worden en om de HTTP-response op te slaan. Wappalyzer is aangepast om aanvullende technieken te detecteren, de volledige HTTP-response naar Explorer te communiceren en om het resultaat in een formaat te retourneren wat door Explorer geïnterpreteerd kan worden[6]. De body van de HTTP-response van de Wappalyzerlookup wordt door Explorer gescand op nieuwe subdomeinen.

Wanneer Drupal, TYPO3, WordPress, Joomla, MediaWiki of phpMyAdmin door Wappalyzer gedetecteerd wordt[7], zal vervolgens met met BlindElephant[8] gericht gepoogd worden de exacte versie van de webapplicatie te achterhalen[9].

[5]Beschikbaar via: https://github.com/ElbertF/Wappalyzer

[6]Verder zijn aanpassingen gemaakt zodat de Location response header alleen gevolgd wordt wanneer deze binnen hetzelfde domein valt. Hiermee wordt voorkomen dat applicaties dubbel gefingerprint worden.

[7]Tevens dient niet HTTP status code 301-303 gedetecteerd te zijn. Dit is wederom om te voorkomen dat een andere applicatie gefingerprint wordt.

[8]Beschikbaar via: http://blindelephant.sourceforge.net

[9]De vereiste versiedatabases van BlindElephant zijn volledig up-to-date gemaakt om meest recente versies te kunnen detecteren.

5 Resultaten

Kwetsbaarheden zijn ingeschaald door gebruik te maken van de security advisory van de betreffende softwareleverancier en CVE-pagina's[10] met bijbehorende CVSS-scores[11]. Bij alle resultaten wordt vermeld op basis waarvan kwetsbaarheden zijn ingeschaald. Er wordt gebruik gemaakt van de impact ratings 'laag' (CVSS 0.0 - 3.9) , 'medium' (CVSS 4.0 - 6.9), 'hoog' (CVSS 7.0 - 8.9), 'kritisch' (CVSS 9.0 - 10.0).

Indien een softwareversie niet meer ondersteund wordt door de producent (End of Life status genoemd) wordt deze gelabeld als "Niet meer ondersteund, kritisch". Voor niet ondersteunde versies worden geen security updates meer uitgebracht. In dit geval is het zaak de software zo snel mogelijk te updaten naar een ondersteunde versie.

Gemeenten worden niet bij naam genoemd, systemen met een hoge en kritische impact rating zijn zowel bij grote als kleine gemeenten aangetroffen.

5.1 Overzicht

Bij 35 van de 417 onderzochte gemeentelijke domeinen was het mogelijk een DNS zone transfer uit te voeren. Hierdoor zijn in totaal door middel van een zone transfer 599 subdomeinen gevonden. In totaal werden 5271 domeinen gevonden. 4729 domeinen bleken actief te zijn. Actief houdt in dat op het achterliggende IP-adres services gedetecteerd zijn.

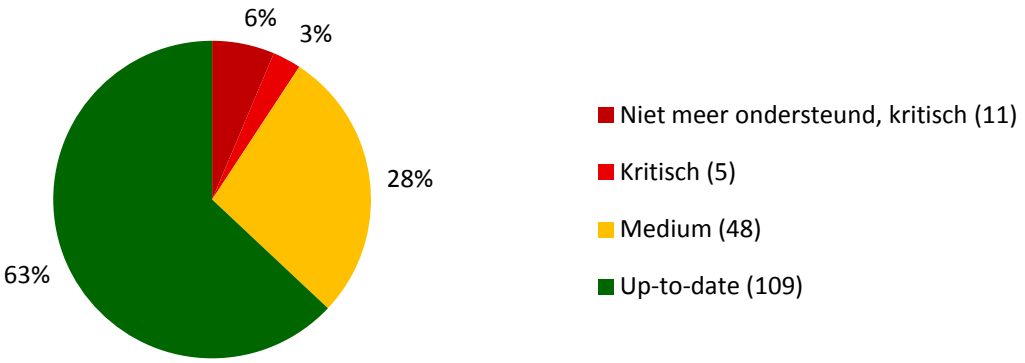
5.2 Webapplicaties

Sommige webapplicaties zijn zowel via poort 443 (HTTPS) en poort 80 (HTTP) te bereiken. Om een dubbele vermelding van een applicatie in de resultaten te voorkomen is getracht na te gaan of de applicaties op beide poorten van hetzelfde domein overeenkomen door de gedetecteerde versie en de body van de HTTP-response te vergelijken[12]. Wanneer de versie en de body overeenkomen wordt een van de applicaties niet meegeteld. Echter kan niet met zekerheid nagegaan worden of het daadwerkelijk om dezelfde applicatie gaat.

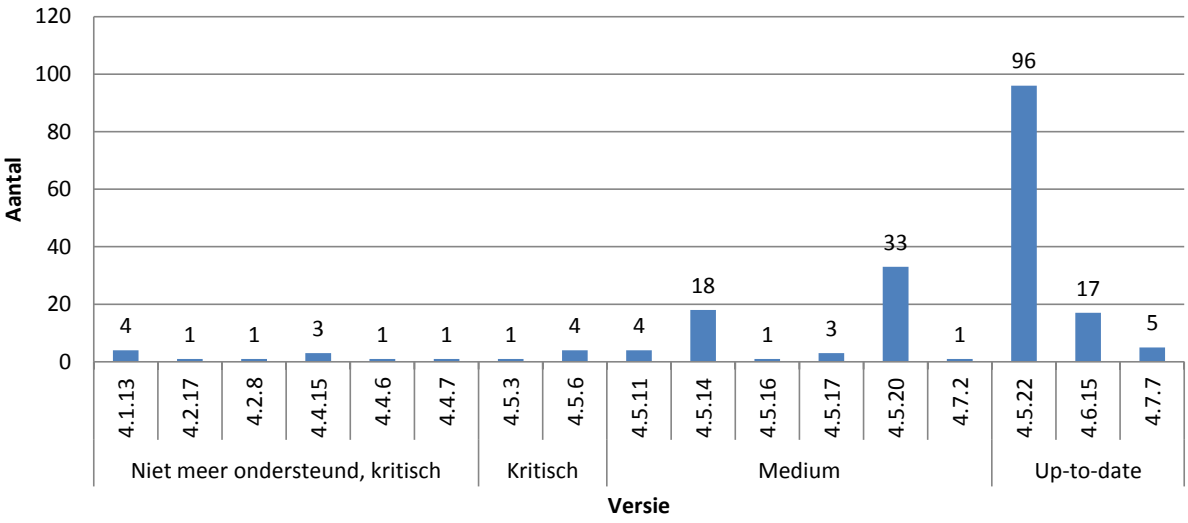
[10] Een CVE-pagina is een beschrijving van een bekende kwetsbaarheid.
[11] De CVSS-score is een indelingsstandaard voor de impact van een kwetsbaarheid.
[12] Om de body van de responses met elkaar te kunnen vergelijken zijn variabele elementen zoals timestamps en het protocol van de webapplicatie uit de body gefilterd. Vervolgens wordt over de licht gestripte body een hashwaarde berekend. De hashwaardes zijn met elkaar vergeleken.

5.2.1 TYPO3

Kwetsbaarheden zijn ingeschaald aan de hand van de TYPO3 Security Advisory: http://typo3.org/teams/security/security-bulletins/typo3-core. Impact scores van de TYPO3 security advisories zijn gerelateerd aan een CVSS-score.



Figuur 1: versiestatus TYPO3



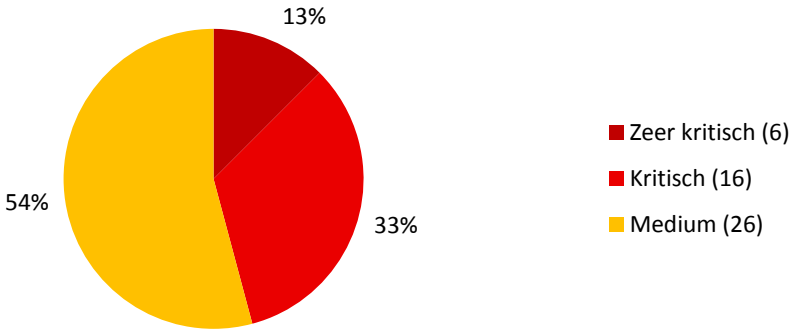
Figuur 2: versiespreiding TYPO3

TYPO3gem is een gemeentelijke gebruikersvereniging rondom het open source CMS TYPO3. TYPO3gem heeft het onderwerp beveiliging hoog op de agenda staan, zo worden onder andere beveiligingsworkshops georganiseerd[13]. Dit lijkt zijn vruchten af te werpen gezien TYPO3-gemeenten meer up-to-date zijn vergeleken met gemeenten met andere CMS'en.

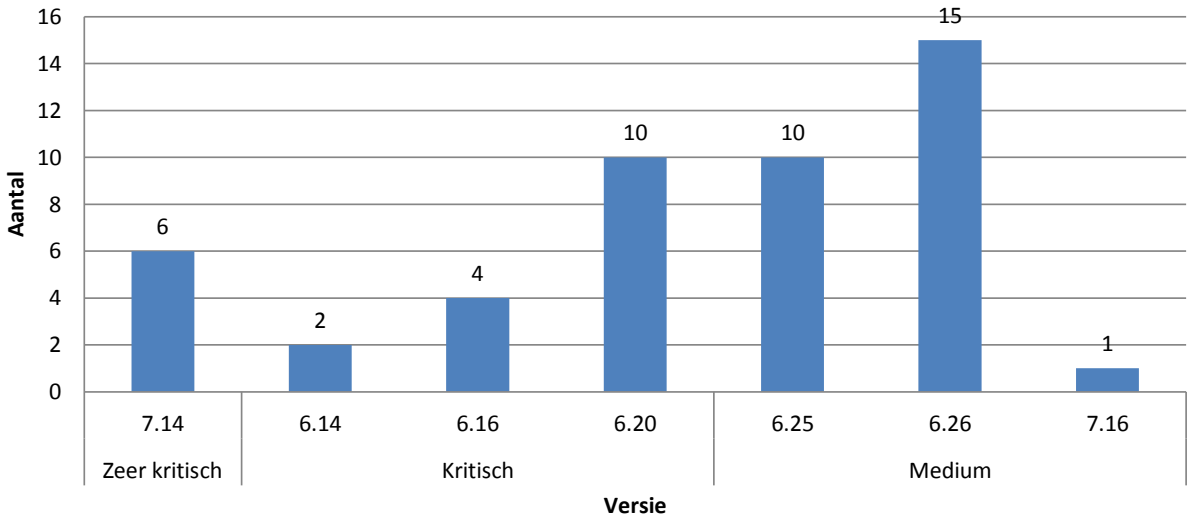
[13] Zie: http://www.typo3gem.nl/index.php?id=63&tx_ttnews[tt_news]=109&cHash=f0299a89d5f4fccf672740061fde1473

5.2.2 Drupal

Kwetsbaarheden zijn ingeschaald aan de hand van de Drupal Security Advisory: http://drupal.org/security. Impact scores staan op deze pagina uiteengezet: http://drupal.org/security-team/risk-levels.



Figuur 3: versiestatus Drupal

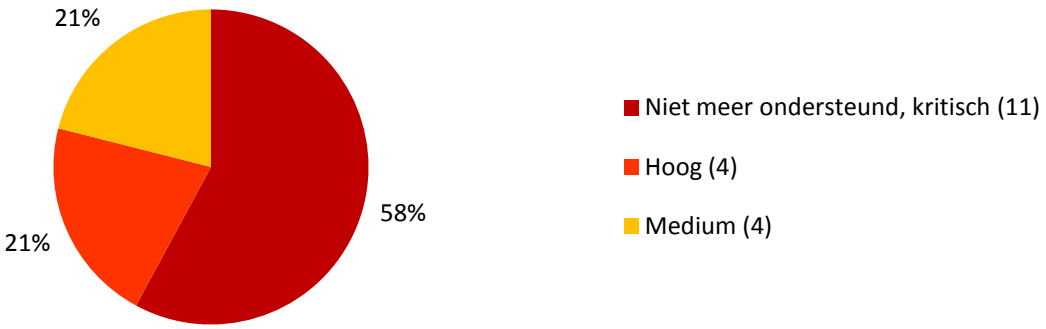


Figuur 4: versiespreiding Drupal

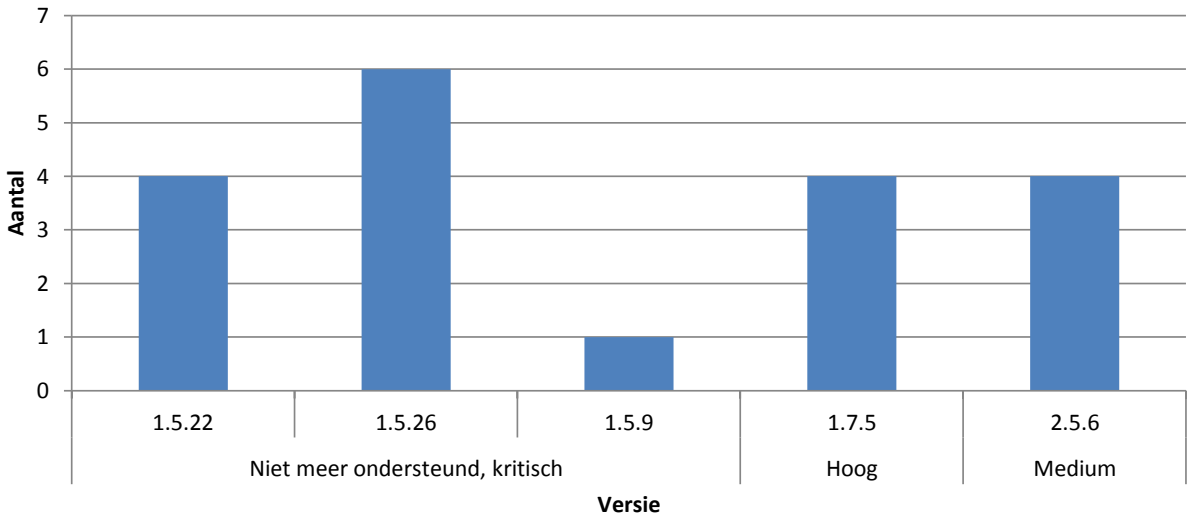
Versie 6.26 (bevat medium kwetsbaarheid) werd 15 maal gedetecteerd. De meest up-to-date versie, 6.27, was uitgebracht op 19 december. Dit betekent dat deze versies op moment van onderzoek vier dagen niet up-to-date waren.

5.2.3 Joomla

Kwetsbaarheden zijn ingeschaald aan de hand van de Joomla-security-pagina: http://developer.joomla.org/security/news/. Impact scores op de Joomla security pagina zijn gerelateerd aan een CVSS-score.



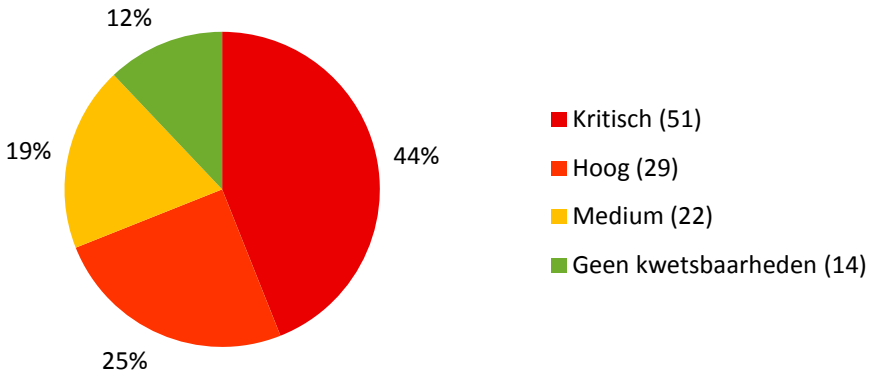
Figuur 5: versiestatus Joomla



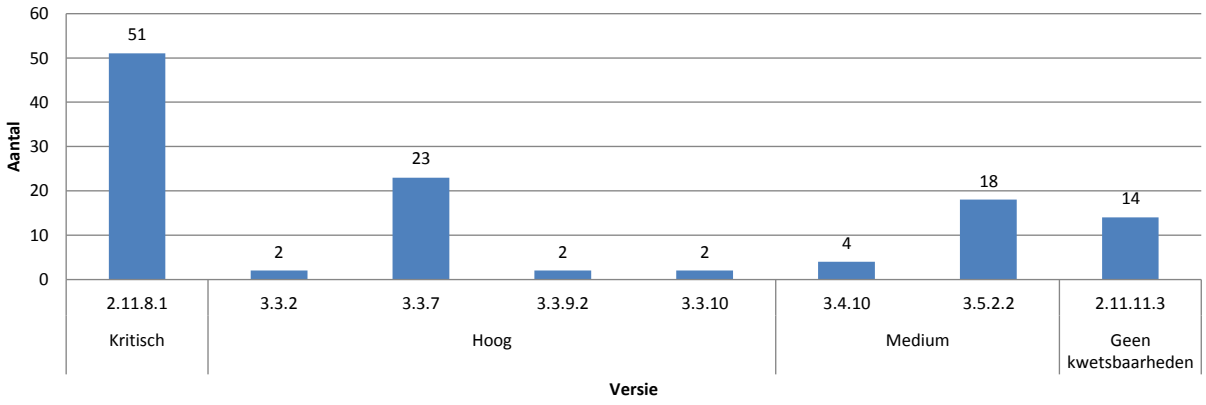
Figuur 6: versiespreiding Joomla

5.2.4 phpMyAdmin

Kwetsbaarheden zijn ingeschaald aan de hand van diverse CVE-pagina's: http://www.cvedetails.com/version-list/784/1341/1/Phpmyadmin-Phpmyadmin.html.



Figuur 7: versiestatus phpMyAdmin



Figuur 8: versiespreiding phpMyAdmin

5.2.5 Overige

Dit hoofdstuk beschrijft applicaties die minder vaak aangetroffen werden.

Owncloud

Owncloud werd in totaal vijf keer gedetecteerd. Drie hiervan bleken op versie 3.0 te draaien welke kritische kwetsbaarheden bevat. Bij de overige twee werd versie 4.5 gedetecteerd, deze versie bevat kwetsbaarheden met een medium impact rating.

MediaWiki

MediaWiki werd één keer aangetroffen. Versie 1.12.0 werd gedetecteerd welke kwetsbaarheden bevat met een hoge impact rating.

Moodle

Moodle werd één keer aangetroffen. Versie 1.9.7 werd gedetecteerd welke kwetsbaarheden bevat met een hoge impact rating.

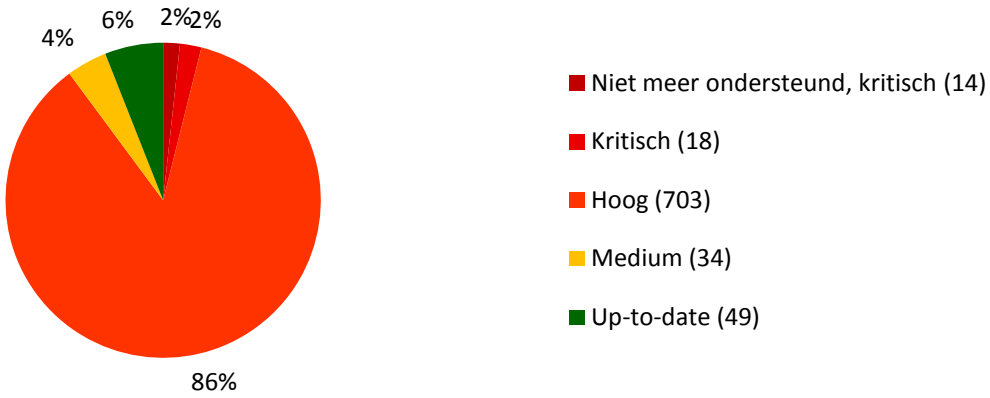
Wordpress

Wordpress werd één keer aangetroffen. Versie 3.4.2 werd gedetecteerd welke kwetsbaarheden bevat met een medium impact rating.

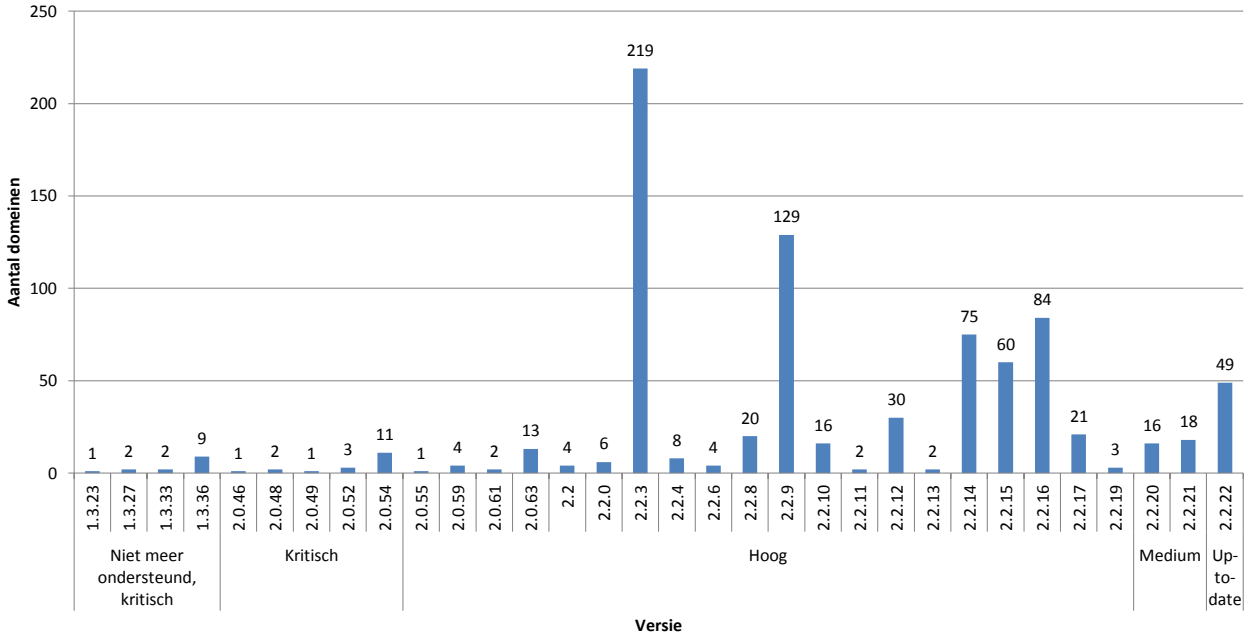
5.3 Webservices

5.3.1 Apache

Kwetsbaarheden zijn ingeschaald aan de hand van de Apache Security Advisory (http://httpd.apache.org/security/) en diverse CVE-pagina's (http://www.cvedetails.com/version-list/45/66/1/Apache-Http-Server.html). Er zijn alleen hoofdversies gedetecteerd (zonder aanduiding van een eventuele package update van een linuxdistributie). Zoals vermeld in hoofdstuk 3 is daarom geen rekening gehouden met package updates. Dit zal het beeld vertekenen. Bijvoorbeeld gedetecteerde versies 2.2.3 (aangemerkt als important, updates in rhel 5/centos 5), 2.2.15 (important, rhel 6/centos 6) en 2.2.16 (important, debian 6) zijn mogelijk niet kwetsbaar.



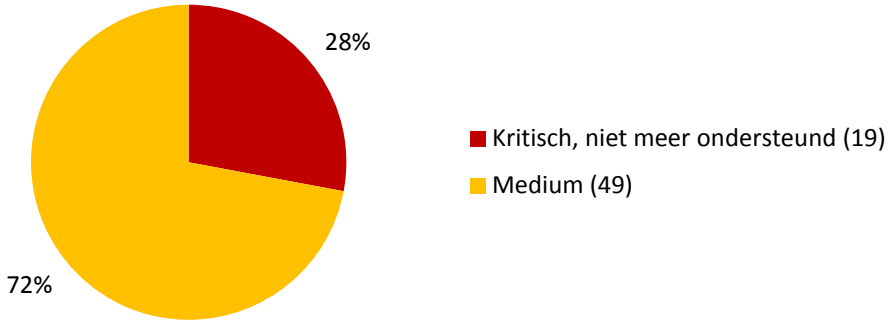
Figuur 9: versiestatus Apache



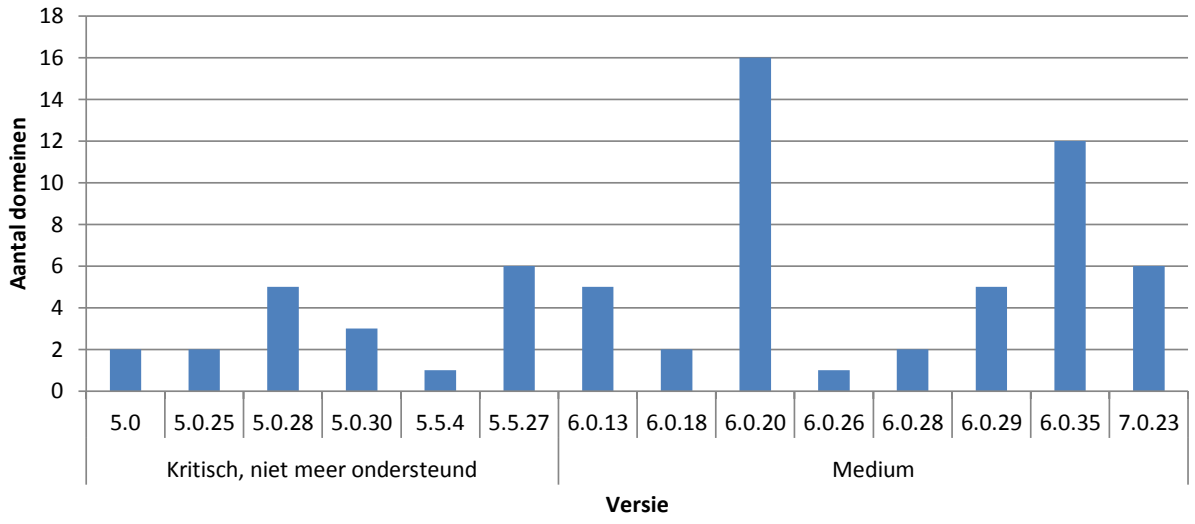
Figuur 10: versiespreiding Apache

5.3.2 Apache Tomcat

Kwetsbaarheden zijn ingeschaald aan de hand van de Apache Tomcat Security Advisory (http://tomcat.apache.org/security.html) en diverse CVE-pagina's (http://www.cvedetails.com/version-list/45/887/1/Apache-Tomcat.html). CVE-2011-3190 en CVE-2009-3548 zijn niet in de resultaten opgenomen omdat de kans klein werd geacht dat gescande systemen daadwerkelijk kwetsbaar zouden zijn. Weer zijn alleen hoofdversies gedetecteerd en is daarom geen rekening gehouden met package updates uit linuxdistributies, hetgeen het beeld zal vertekenen. Bijvoorbeeld gedetecteerde versie 6.0.35 (aangemerkt als medium, updates in debian 6) is mogelijk niet kwetsbaar. Mogelijke up-to-date versie 6.0.24 voor rhel 6/centos 6 is niet aangetroffen.



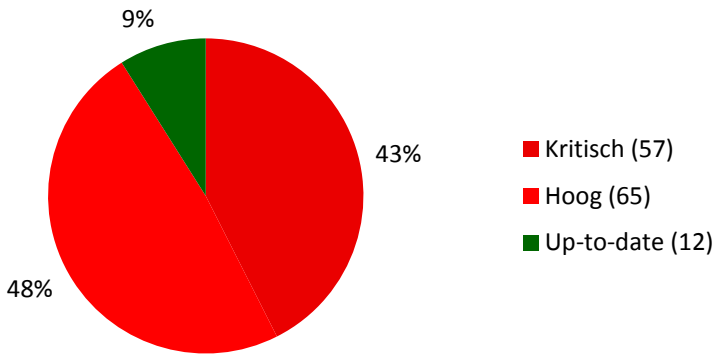
Figuur 11: versiestatus Apache Tomcat



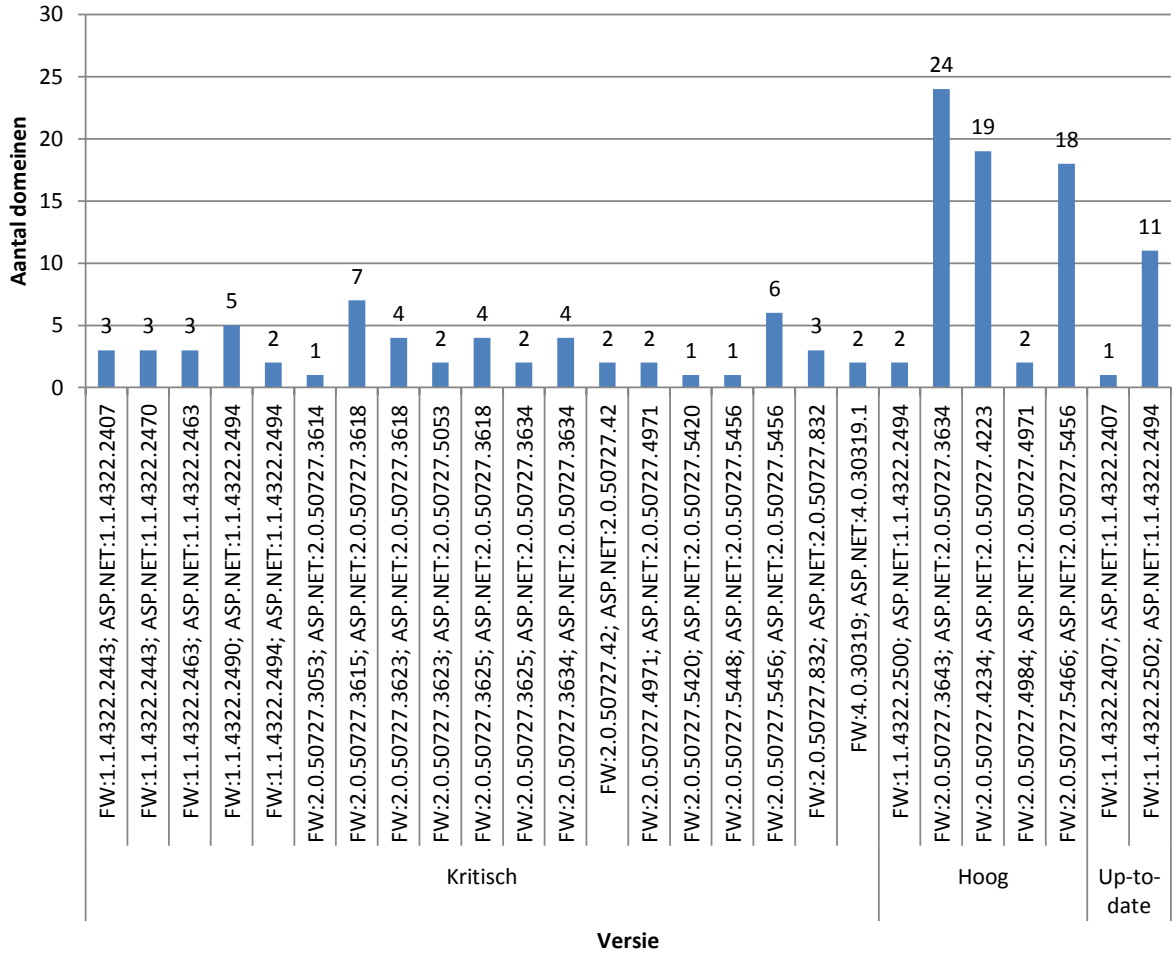
Figuur 12: versiespreiding Apache Tomcat

5.3.3 ASP.NET

Kwetsbaarheden zijn ingeschaald aan de hand van Microsoft Security Bulletins (http://technet.microsoft.com/en-us/security/bulletin).



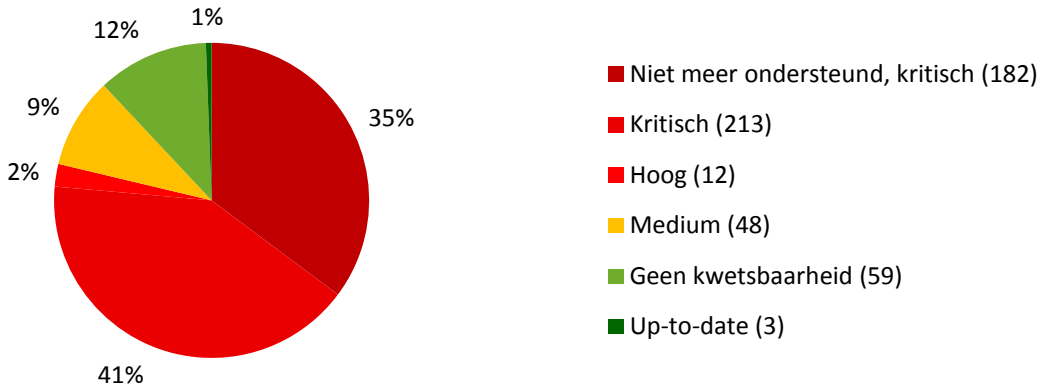
Figuur 13: versiestatus ASP.NET



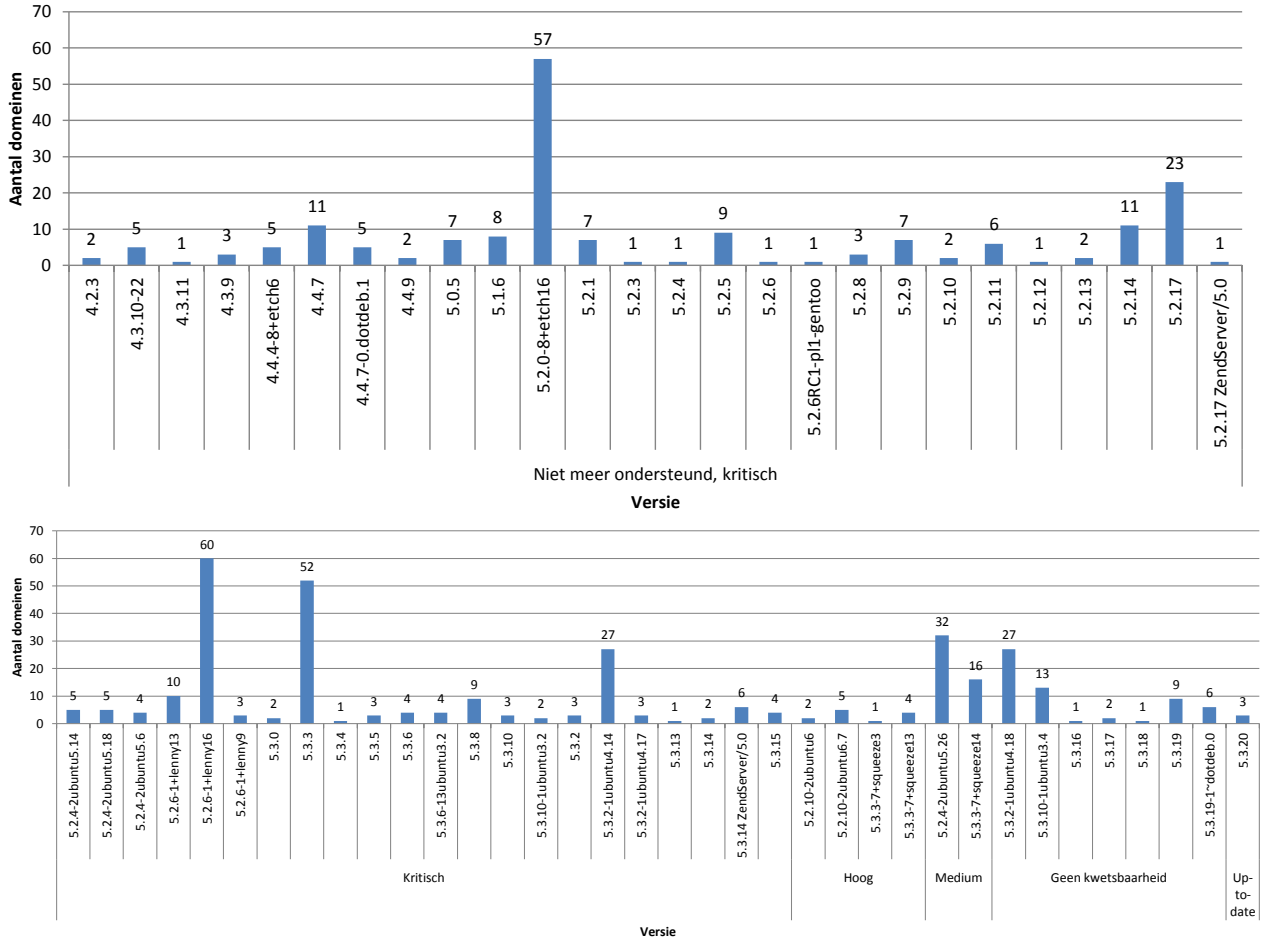
Figuur 14: versiespreiding ASP.NET

5.3.4 PHP

Kwetsbaarheden zijn ingeschaald aan de hand van diverse CVE-pagina's (http://www.cvedetails.com/version-list/74/128/1/PHP-PHP.html). De gedetecteerde versie bevat soms een aanduiding voor een (m.n. debian/ubuntu) package update en aan de hand daarvan is dan de kwetsbaarheid vastgesteld. Dit is echter niet altijd het geval. Toch kan het zijn dat er package updates zijn toegepast. Bijvoorbeeld gedetecteerde versies 5.1.6 (aangemerkt als "niet meer ondersteund, kritisch"maar er worden nog backported security updates geleverd voor rhel 5/centos 5) en 5.3.3 (kritisch, rhel 5/centos 5/rhel 6/centos 6) zijn mogelijk niet kwetsbaar.



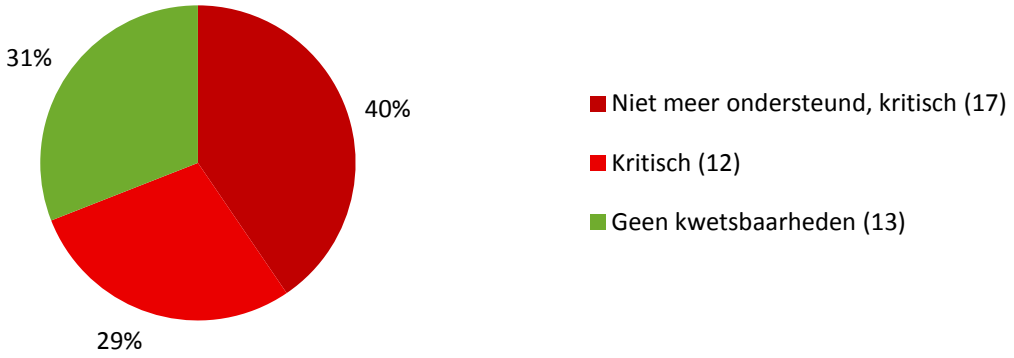
Figuur 15: versiestatus PHP



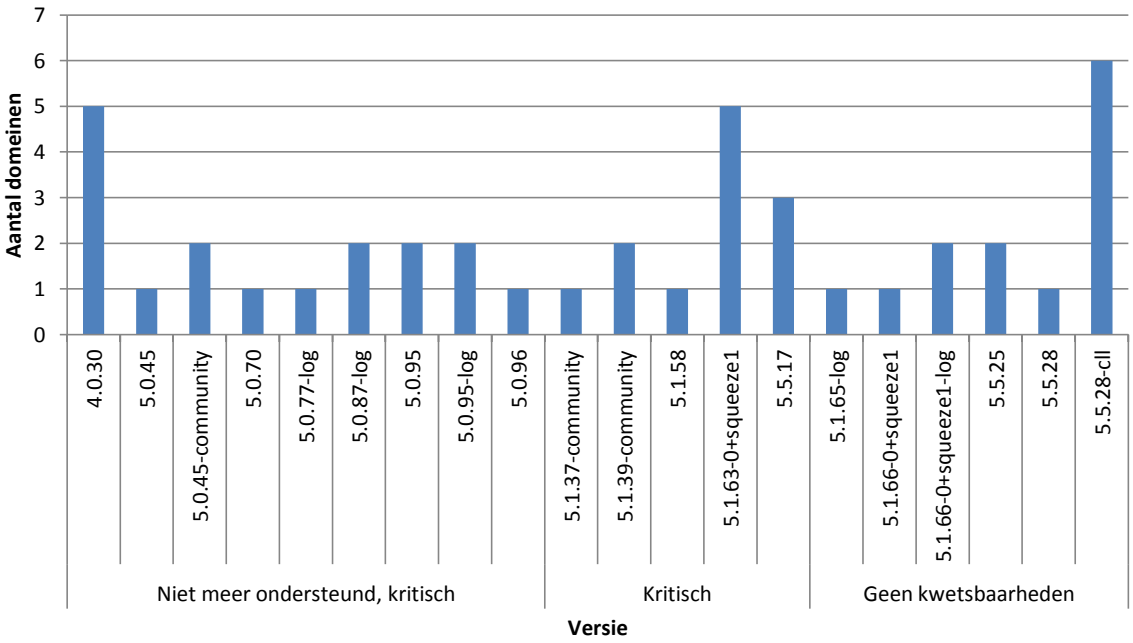
Figuur 16: versiespreiding PHP

5.3.5 MySQL

Kwetsbaarheden zijn ingeschaald aan de hand van diverse CVE-pagina's (http://www.cvedetails.com/version-list/185/316/1/Mysql-Mysql.html). De gedetecteerde versie bevat soms een aanduiding voor een package update en aan de hand daarvan is de kwetsbaarheid vastgesteld. Dit is echter niet altijd het geval. Toch kan het zijn dat er package updates zijn toegepast. Bijvoorbeeld gedetecteerde versie 5.0.95 (of 5.0.95-log, aangemerkt als "niet meer ondersteund, kritisch"maar er worden nog backported security updates geleverd voor rhel 5/centos 5) is mogelijk niet kwetsbaar.



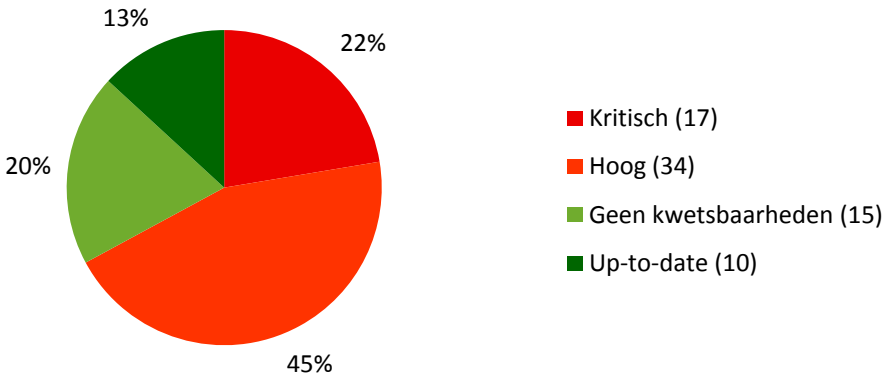
Figuur 17: versiestatus MySQL



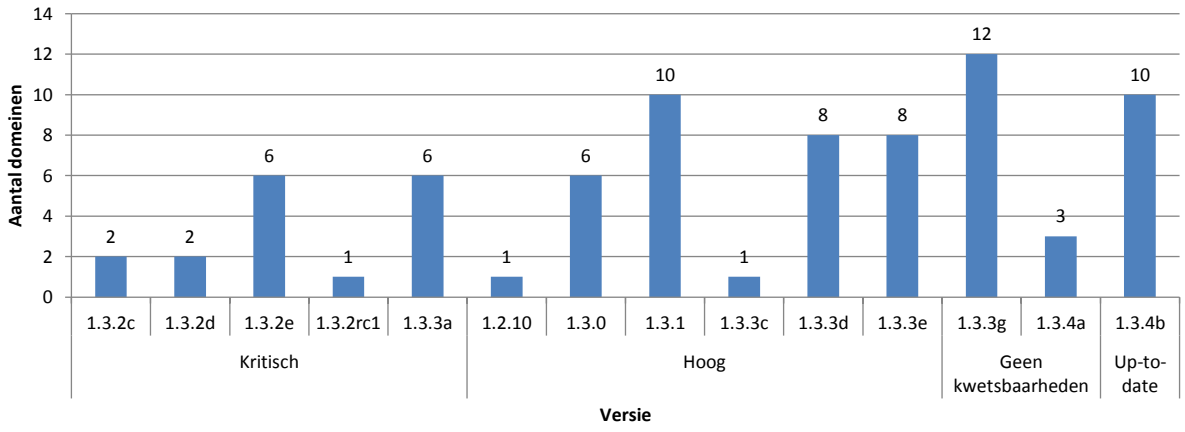
Figuur 18: versiespreiding MySQL

5.3.6 ProFTPD

Kwetsbaarheden zijn ingeschaald aan de hand van diverse CVE-pagina's (http://www.cvedetails.com/version-list/9520/16873/1/Proftpd-Proftpd.html). Er zijn alleen hoofdversies gedetecteerd en is daarom geen rekening gehouden met package updates, hetgeen het beeld kan vertekenen. Bijvoorbeeld gedetecteerde versie 1.3.3a (aangemerkt als hoog, updates in debian 6) is mogelijk niet kwetsbaar.



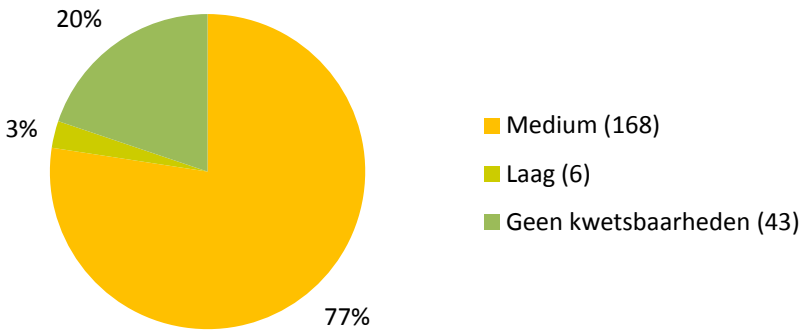
Figuur 19: versiestatus ProFTPD



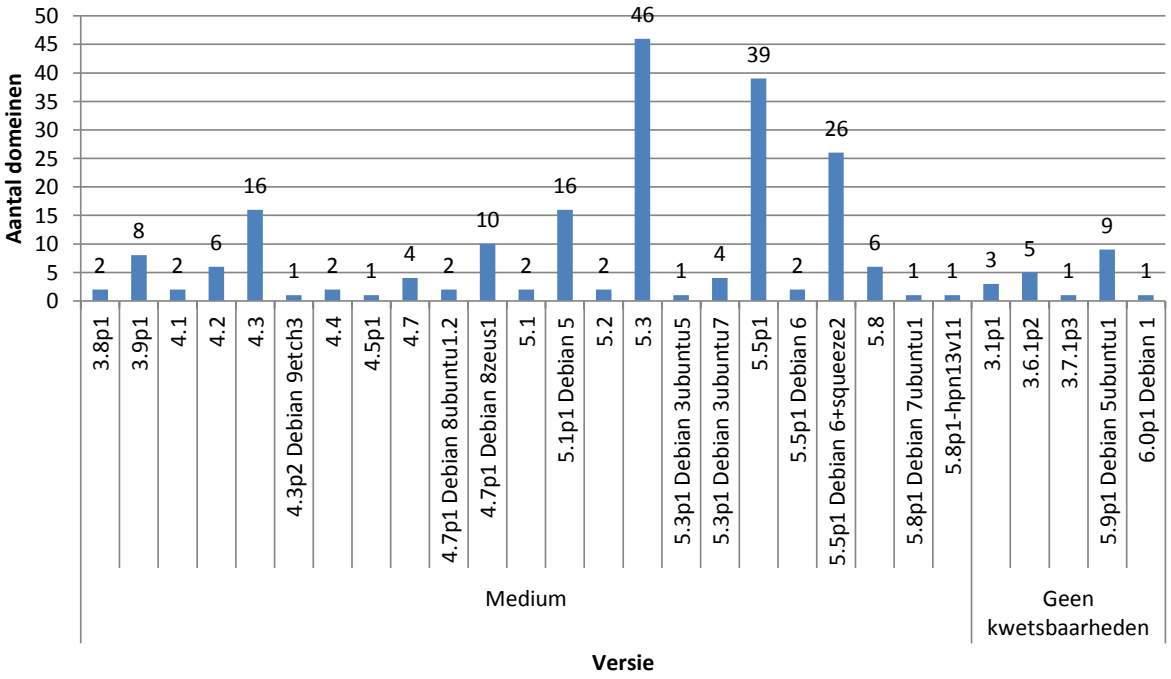
Figuur 20: versiespreiding ProFTPD

5.3.7 OpenSSH

Kwetsbaarheden zijn ingeschaald aan de hand van diverse CVE-pagina's (http://www.cvedetails.com/version-list/7161/12081/1/Openssh-Openssh.html). CVE-2010-4478 is niet in de resultaten opgenomen. Dit gaat om een kwetsbaarheid met een impact rating 'hoog' die in alle versies voor OpenSSH 5.6 aanwezig is. Het J-PAKE protocol waar deze kwetsbaarheid in aanwezig is, is echter als experimenteel opgenomen in OpenSSH. Daarom zal het waarschijnlijk niet ingeschakeld zijn in distributies. De gedetecteerde versie bevat soms een aanduiding voor een (m.n. debian/ubuntu) package update en aan de hand daarvan is dan de kwetsbaarheid vastgesteld. Dit is echter niet altijd het geval. Toch kan het zijn dat er package updates zijn toegepast. Bijvoorbeeld gedetecteerde versies 4.3 (aangemerkt als medium, updates in rhel 5/centos 5) en 5.3 (medium, rhel 6/centos 6) zijn mogelijk niet kwetsbaar.



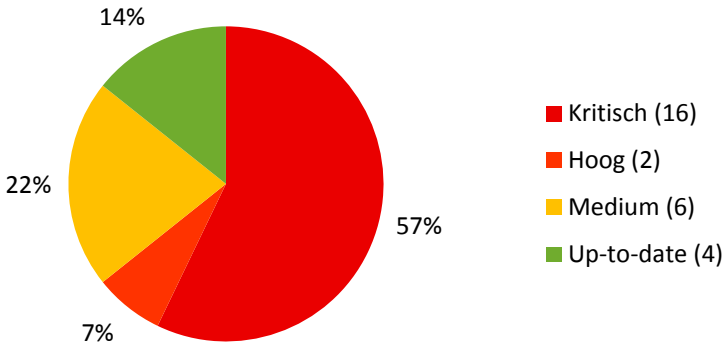
Figuur 21: versiestatus (zonder CVE-2010-4478) OpenSSH



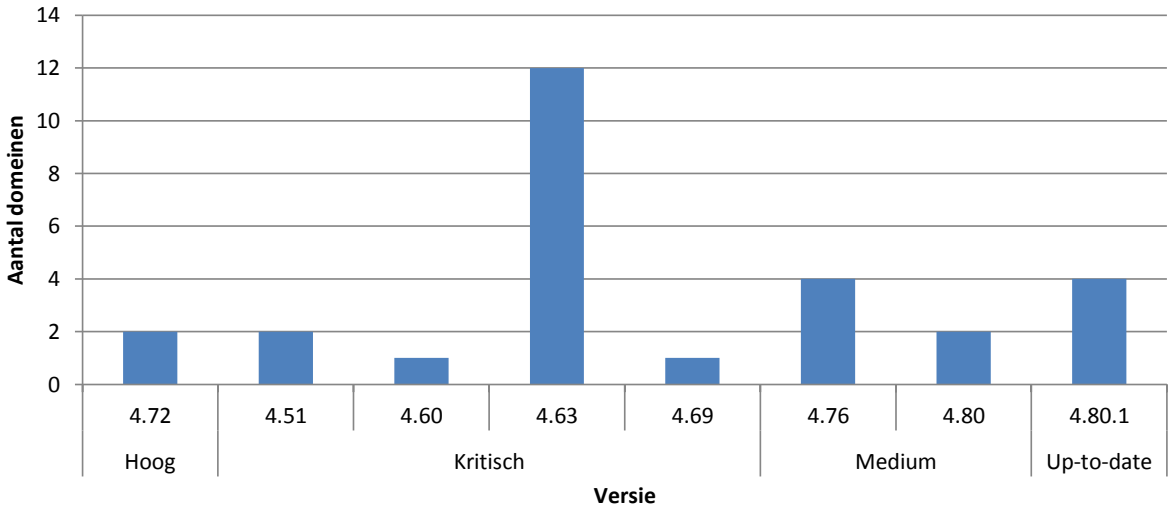
Figuur 22: versiespreiding OpenSSH

5.3.8 Exim

Kwetsbaarheden zijn ingeschaald aan de hand van diverse CVE-pagina's (http://www.cvedetails.com/version-list/10919/19563/1/Exim-Exim.html). Er zijn alleen hoofdversies gedetecteerd en is daarom geen rekening gehouden met package updates, hetgeen het beeld kan vertekenen. Bijvoorbeeld gedetecteerde versies 4.63 (aangemerkt als kritisch, updates in rhel 5/centos 5) en 4.72 (hoog, debian 6) zijn mogelijk niet kwetsbaar.



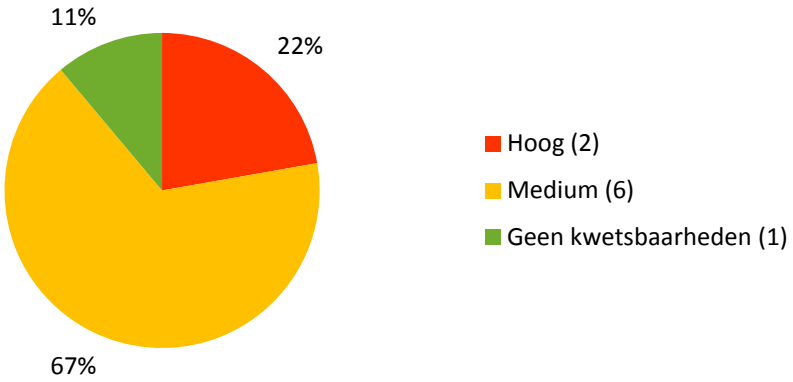
Figuur 23: versiestatus Exim



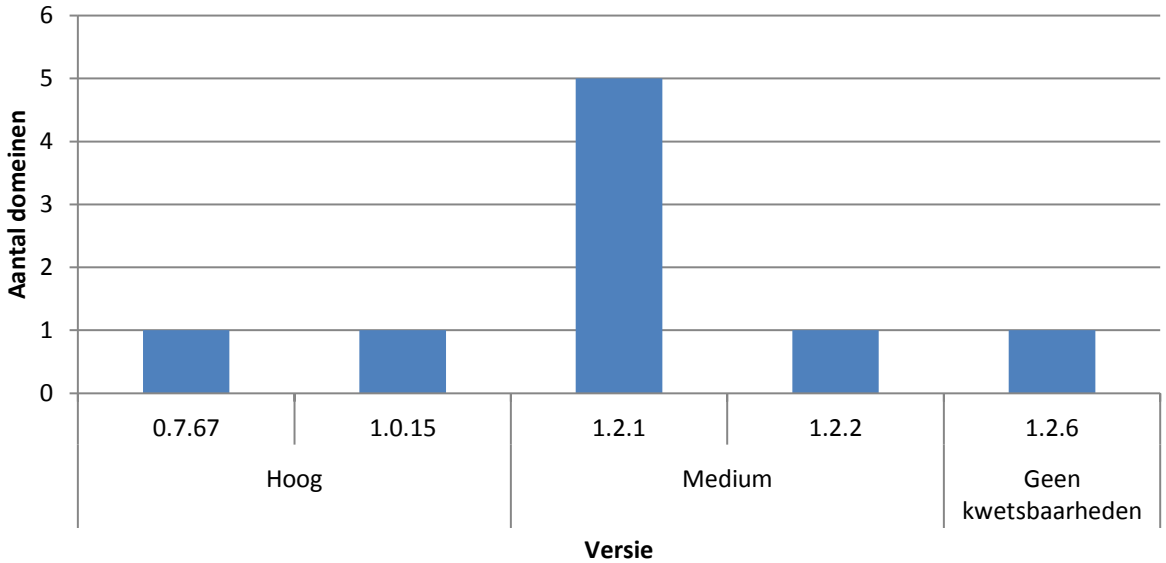
Figuur 24: versiespreiding Exim

5.3.9 Nginx

Kwetsbaarheden zijn ingeschaald aan de hand van diverse CVE-pagina's (http://www.cvedetails.com/version-list/10048/17956/1/Nginx-Nginx.html). Er zijn alleen hoofdversies gedetecteerd en is daarom geen rekening gehouden met package updates, hetgeen het beeld kan vertekenen. Bijvoorbeeld gedetecteerde versie 0.7.67 (aangemerkt als hoog, updates in debian 6) is mogelijk niet kwetsbaar.



Figuur 25: versiestatus Nginx



Figuur 26: versiespreiding Nginx

5.3.10 Overige

Dit hoofdstuk beschrijft software die minder vaak aangetroffen werden.

Microsoft IIS

Microsoft IIS werd totaal 766 keer gedetecteerd. Versie 5.0 (geleverd bij Windows 2000) werd op 10 domeinen gedetecteerd. Windows 2000 wordt sinds 2010 niet meer ondersteund door Microsoft, deze versie heeft daarom een kritische impact rating. Uit de data van de overige versies kan niet bepaald worden welke kwetsbaarheden van toepassing zijn.

Sendmail

Op vier servers werd Sendmail gedetecteerd (versies: 8.13.8, 8.14.0, 8.14.3, 8.14.3) met kwetsbaarheden met een hoge impact rating. Aan de IP-adressen zijn 4 domeinen gekoppeld. Er zijn alleen hoofdversies gedetecteerd en is daarom geen rekening gehouden met package updates, hetgeen het beeld kan vertekenen. Bijvoorbeeld gedetecteerde versie 8.13.8 (rhel 5/centos 5) en 8.14.3 (debian 6) zijn mogelijk niet kwetsbaar.

Lotus Domino SMTPD

Op drie servers werd Lotus Domino gedetecteerd (versies: 8.13.8, 8.14.0, 8.14.3, 8.14.3) met kwetsbaarheden met een kritische impact rating. Aan de IP-adressen zijn 6 domeinen gekoppeld.

Oracle Application Server

Op twee servers werd Oracle Application Server gedetecteerd (versies: 0.1.3.1.0, 10.1.2.0.2) met kwetsbaarheden met een kritische impact rating. Aan de IP-adressen zijn twee domeinen gekoppeld.

Guild FTPd

Guild FTPd werd op één server gedetecteerd waaraan één domein gekoppeld is. Versie 0.999.14 werd gedetecteerd, deze versie bevat kwetsbaarheden met een kritische impact rating.

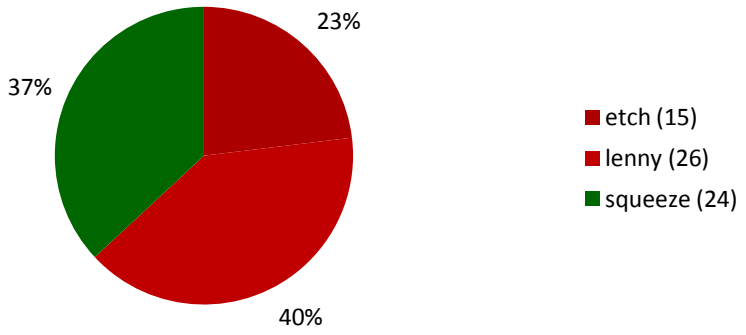
WS FTPd

WS FTPd werd op één server gedetecteerd waaraan twee domeinen gekoppeld zijn. Versie 4.0.2 werd gedetecteerd, deze versie bevat kwetsbaarheden met een hoge impact rating.

5.4 Operating systems

Het komt voor dat aan de hand van de banner van een request response, behalve de versie van de webservice, ook die van het onderliggende operating system (OS) te achterhalen valt. Zo kan bijvoorbeeld worden vastgesteld dat er voor het OS geen security updates meer worden verstrekt. Dit heeft uiteraard grote consequenties voor de veiligheid van het systeem. Het tijdstip dat een OS niet meer zal worden ondersteund wordt normaliter ruimschoots van tevoren en breed bekend gemaakt.

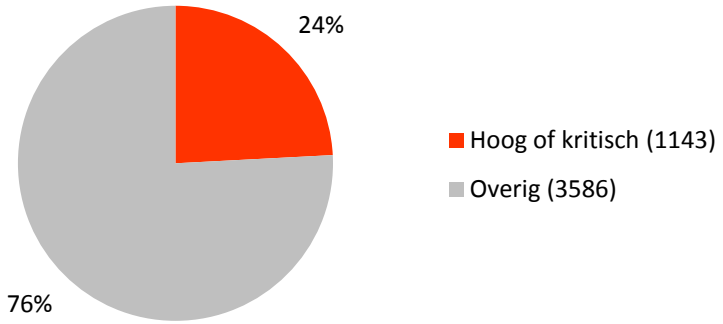
Met name voor de stable releases van het Debian OS valt de versie geregeld vast te stellen. Ten tijde van het onderzoek is slechts huidige stable release squeeze ondersteund. Voorgangers ontvangen geen security updates: etch niet sinds februari 2010 en lenny niet sinds februari 2012. Voor 45 systemen (ip-adressen) valt zo vast te stellen dat het OS achterhaald is. Om dit in perspectief te plaatsen, is voor Debian een vergelijk gemaakt tussen de aangetroffen stable releases.



Figuur 27: Gedetecteerde Debian stable versies (per ip-adres).

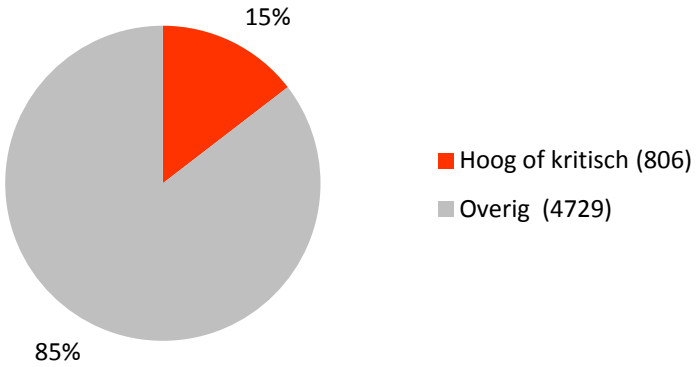
5.5 Totaalimpact

Kwetsbaarheden kunnen verstrekkende gevolgen voor de betrouwbaarheid, integriteit en vertrouwelijkheid van het hele systeem. Dit betekent dat *alle* domeinen die beschikbaar zijn op het betreffende systeem (volgens aanname hetzelfde IP-adres) mogelijk ook kwetsbaar zijn. In onderstaande afbeelding 28 is weergegeven hoeveel domeinen ten opzichte van alle actieve domeinen mogelijk kwetsbaar zijn door aangetroffen kwetsbaarheden met een hoge en kritische kwetsbaarheid op het systeem.



Figuur 28: Totaalimpact op alle domeinen door kwetsbaarheden met een hoge en kritische impact rating.

Zoals eerder vermeld kan niet met zekerheid gezegd worden of een gedetecteerde versie ook daadwerkelijk kwetsbaar is en kan dit met name door package updates tot een vertekend beeld leiden. Om dit nader te onderzoeken, is beschouwd wat gebeurt als de bij de webservices (zie sectie 5.3) genoemde versies buiten beschouwing gelaten worden. Het resultaat is te zien in afbeelding 29. De uitgesloten versies vormen echter niet een uitputtende lijst van mogelijk niet-kwetsbare versies. Hierdoor kan het aandeel hoog/kritisch kwetsbare domeinen lager uitvallen. Voor de analyse wordt aangenomen dat de uitgesloten versies alle up-to-date zijn. Dus dat beheer bijvoorbeeld altijd via packages van een ondersteunde linuxdistributie gaat en dat in ieder geval alle beschikbare hoge/kritische security updates zijn toegepast. Mocht dit niet waar zijn, dan kan het aandeel hoog/kritisch kwetsbare domeinen hoger uitvallen.



Figuur 29: Totaalimpact op alle domeinen door kwetsbaarheden met een hoge en kritische impact rating, eerder genoemde webserviceversies buiten beschouwing gelaten.

In het algemeen moet worden opgemerkt dat zeer frequent in het geheel geen versie is vastgesteld: bij de port scans in meer dan 85% van de gevallen. Hierdoor kan het aantal domeinen op een server met kwetsbaarheid met hoge en kritische impact rating in werkelijkheid aanmerkelijk hoger zijn.

6 Vervolgonderzoek

In samenwerking met gemeenten zou dit onderzoek uitgebreid kunnen worden met alle domeinen en bijbehorende subdomeinen die gemeenten in hun bezit hebben. Bij dit onderzoek hebben wij slechts het hoofddomein (bijv. amsterdam.nl) als uitgangspunt gebruikt. Bij pentesten wordt de scope van het onderzoek vaak beperkt tot de belangrijkste systemen. Het is echter mogelijk dat een belangrijk en veilig bevonden systeem indirect kwetsbaar is via veel minder significante systemen. Denk bijvoorbeeld aan gebruikers die op verschillende systemen hetzelfde wachtwoord gebruiken.

Vaak kunnen de functionaliteiten van een webapplicatie met extensies/modules verder uitgebreid worden. Naast de core van de webapplicatie is het net zo belangrijk dat alle extra extensies/modules tijdig geüpdate worden. Het is goed mogelijk dat webapplicaties die in dit onderzoek up-to-date zijn bevonden, alsnog kwetsbaar zijn via een extensie/module. Het is daarom interessant om applicaties verder fingerprinten door ook extensies/modules in het onderzoek mee te nemen.

Verder zou Explorer uitgebreid kunnen worden om bijvoorbeeld meer software te detecteren en te fingerprinten of zouden checks ingebouwd kunnen worden om configuratiefouten te detecteren. Daarnaast zouden meer open source tools gekoppeld kunnen worden, denk bijvoorbeeld aan intrusievere tools als SQLmap om SQL-injecties te detecteren.

Door eenzelfde onderzoek hierna periodiek uit te voeren kan bezien worden hoe effectief gevoerd beleid is. Explorer kan uitgebreid worden qua rapportagemogelijkheden. Zo kan inzichtelijk worden gemaakt hoeveel tijd services/webapplicaties achterlopen qua updates. Het gemiddelde hiervan per service is bijvoorbeeld een interessant kengetal.

7 Conclusie

Door middel van een script waarmee een aantal open source tools zijn gekoppeld zijn zo veel mogelijk softwareversies van websystemenen van alle gemeenten in kaart gebracht. Van alle softwareversies die gedetecteerd werden zijn de kwetsbaarheden en bijbehorende impact rating opgezocht.

Wanneer het aantal up-to-date of niet-kwetsbare systemen wordt afgezet tegen het aantal systemen met een kritische of hoge impact rating kan niet anders geconcludeerd worden dan dat ruim een jaar na alle ophef door Lektober nog steeds veel te veel oude software in gebruik is. Deze kritische/hoge kwetsbaarheden treffen zowel grote als kleine gemeenten. Bij een aantal softwarepakketten zoals Drupal, Joomla, phpMyAdmin, ASP.NET en PHP zijn zelfs (bijna) alleen kwetsbare softwareversies aangetroffen. Het probleem lijkt verder structureel: van de gedetecteerde Debian servers lijkt bijna tweederde op een niet meer ondersteunde OS-versie te draaien. 24% van alle gedetecteerde gemeentelijke systemen kan mogelijk beïnvloed worden door de kwetsbaarheden met een hoge of kritische impact rating. De verouderde software op deze systemen zou relatief eenvoudig misbruikt kunnen worden door kwaadwillenden.

Het onderzoek toont aan dat de huidige inspanningen om gemeentelijke systemen te beveiligen nog niet afdoende effect hebben gehad. Men dient continu bewust te zijn van welke systemen aanwezig zijn en welke publiek toegankelijk dienen te zijn. Systemen die niet publiek toegankelijk hoeven te zijn, dienen afgeschermd te worden. Vervolgens dient er focus te liggen op het up-to-date houden van systemen. In het document "ICT beveiligingsrichtlijnen voor webapplicaties"van het Nationaal Cyber Security Centrum staat helder omschreven hoe het updateproces dient plaats te vinden.

Door eenzelfde onderzoek hierna periodiek uit te voeren kan bezien worden hoe effectief gevoerd beleid is.