Centraal Planbureau

Een blik op de NCSC beveiligingsadviezen

Het ministerie van Justitie en Veiligheid heeft het CPB gevraagd datagedreven onderzoek te doen naar de beveiligingsadviezen van het NCSC en daar kwantitatieve inzichten over te verschaffen.

Uit het onderzoek blijkt dat dat er in de afgelopen jaren een redelijk grote toename is geweest van het aantal NCSC-adviezen.

Van deze adviezen worden verreweg de meeste als medium-medium en medium-hoog geclassificeerd: schade door misbruik is waarschijnlijk. Slechts een beperkt aantal adviezen valt in de hoogste risicocategorie. Voor ongeveer 30% van de adviezen bestaan publiek bekende exploits.

CPB Notitie

Freek Ruesink
Rinske Windig

juli 2019

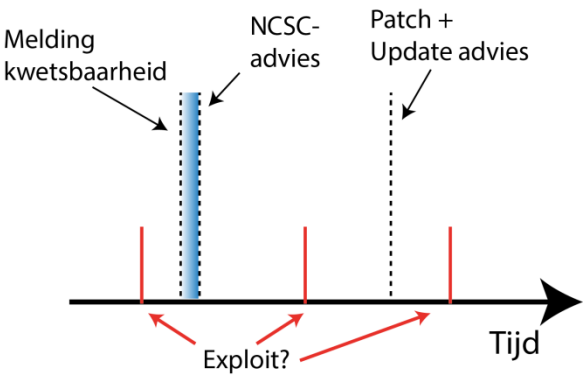
1 Inleiding

Softwarekwetsbaarheden zijn een belangrijke bron van cyberdreigingen. Kwaadwillenden gebruiken softwarekwetsbaarheden om toegang te krijgen tot systemen of deze te verstoren en zo (kritieke) processen te ontregelen of gevoelige data te stelen. Voor een succesvolle aanval is wel exploitcode nodig: programmeercode die erop is gericht om de softwarekwetsbaarheid uit te buiten. De notPetya ransomware-aanval in 2017, waar onder andere de Rotterdamse haven problemen van ondervond, is een voorbeeld waarbij exploitcode een kwetsbaarheid misbruikte met ernstige gevolgen als resultaat.

In Nederland is het NCSC de centrale organisatie op het gebied van cyberveiligheid. Een van de kerntaken van het NCSC is om te reageren op cyberdreigingen en incidenten die invloed kunnen hebben op de Rijksoverheid en vitale processen in Nederland[1]. Een vitaal proces wordt gekenmerkt doordat uitval ervan grote economische, fysieke of sociaal-maatschappelijke gevolgen kent[2]. Het NCSC brengt (onder andere) beveiligingsadviezen uit om organisaties te waarschuwen voor bekende kwetsbaarheden om zo uitval te voorkomen.

Een beveiligingsadvies bevat informatie over een recent gevonden kwetsbaarheid in hard- of software. Daarnaast brengt het NCSC adviesupdates van bestaande adviezen uit wanneer er nieuwe relevante informatie beschikbaar komt (zie ook Figuur 1.1).

Figuur 1.1. Illustratieve tijdlijn van gebeurtenissen



De bron van informatie over de kwetsbaarheid is in veel gevallen een publicatie van een productleverancier of onderzoeker. Een beveiligingsadvies bevat een beschrijving van de kwetsbaarheid, de mogelijke gevolgen en mogelijke oplossingen, en ook of het NCSC exploitcode heeft gesignaleerd. Daarnaast bevat een advies ook een risico-inschatting van de kans dat er misbruik van een kwetsbaarheid wordt gemaakt en de ernst van mogelijke schade[3]. Deze beveiligingsadviezen vormen het hart van ons onderzoek.

[1] De Rijksoverheid en de organisaties die vitale processen beheren worden door het NCSC ook wel aangeduid als doelgroeporganisaties, namelijk die organisaties waar het NCSC-adviezen voor schrijft.
[2] Voor een volledige definitie zie hier.
[3] Voor de werkwijze van het maken van deze inschatting zie hier.

Het ministerie van Justitie en Veiligheid (JenV) heeft het CPB per brief d.d. 27 mei 2019 gevraagd datagedreven onderzoek te doen naar deze beveiligingsadviezen en daar kwantitatieve inzichten over te verschaffen. Hierbij is gevraagd om in te gaan op:

- De ontwikkeling van het aantal adviezen;
- De risico-inschaling van de kwetsbaarheden; en
- De vraag of een betrouwbare koppeling gelegd kan worden tussen beveiligingsadviezen en publiek bekende kwetsbaarheden.

Met deze Notitie, en de Engelse vertaling daarvan, beantwoorden wij dit verzoek van JenV. De Notitie richt zich op de bovenstaande vragen van JenV en kan niet gezien worden als een evaluatie (of een onderdeel daarvan) van de werkzaamheden van het NCSC.

Op basis van ons onderzoek concluderen we dat er in de afgelopen jaren een redelijk grote toename is geweest in het aantal door NCSC gepubliceerde adviezen. Van deze adviezen worden verreweg de meeste als medium-medium en medium-hoog geclassificeerd (waarschijnlijkheid-schade van misbruik). Slechts een beperkt aantal adviezen valt in de hoogste risicocategorie. Het in de adviezen meest genoemde gevolg bij misbruik van een kwetsbaarheid is een Denial of service. Ook keken we naar de vraag of de data verkregen uit de beveiligingsadviezen en een externe exploit database van voldoende kwaliteit zijn om een betrouwbare koppeling tussen die twee te maken. Helaas is dat niet het geval. Zo konden we onder andere niet altijd verifiëren of een exploit legitiem[4] is en zaten er bij een steekproef enkele fouten in de CVE-nummers[5] in de beveiligingsadviezen die we gebruiken voor de koppeling.

[4] Bijvoorbeeld of de exploit daadwerkelijk werkt.
[5] CVE staat voor Common Vulnerabilities and Exposures. CVE-nummers worden toegekend aan publieke soft- en hardware kwetsbaarheden. Algemeen beheer hiervan wordt verzorgd door een publiek-private coöperatie, zie cve.mitre.org.

2 Databronnen

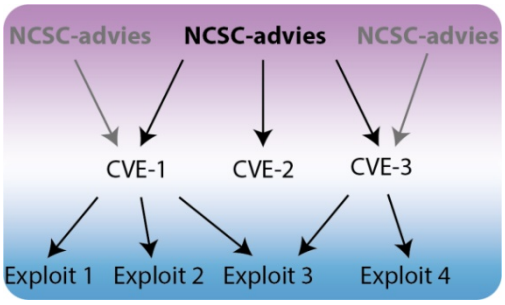
Bij onze analyse maken we gebruik van twee verschillende datasets. Onze primaire dataset bestaat uit alle beveiligingsadviezen uitgebracht door het NCSC tussen januari 2012 en augustus 2018, dit zijn er 14.036. Het is bij ons niet bekend welk vitaal proces er van bepaalde softwarekwetsbaardheden last kan hebben. Zulke informatie is vertrouwelijk. De belangrijkste gegevens die wij uit de adviezen kunnen destilleren zijn:

- De datum van uitgifte van het advies,
- Het advies-ID (een identificatienummer),
- Het versienummer van een advies (1.00, 1.01, ...),
- Op welk(welke) *Operating System(s)* het advies betrekking heeft,
- De betrokken programmatuur,
- De CVE-nummers behorende bij de kwetsbaarheid,
- De kans op misbruik (laag/middel/hoog) zoals door NCSC ingeschaald,
- De ernst van de schade (laag/middel/hoog) die optreedt wanneer de kwetsbaarheid misbruikt wordt, zoals door NCSC ingeschaald,
- De consequentie van misbruik van de kwetsbaarheid (DoS/datalek/uitvoeren van willekeurige code/verkrijgen van rechten/lekkage informatie),
- Of er reeds exploitcode beschikbaar is, en
- Of er een oplossing, bijvoorbeeld een patch, bekend is.

Figuur 2.1. Voorbeeld van een deel van een beveiligingsadvies

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

   ####################################################
  ##  N C S C ~ B E V E I L I G I N G S A D V I E S  ##
 ####################################################

######################## UPDATE 1.02 ##############################

Titel           : Kwetsbaarheid in libssh verholpen
Advisory ID     : NCSC-2015-0002
Versie          : 1.02
Kans            : medium
CVE ID          : CVE-2014-8132
                  (http://cve.mitre.org/cve/)
Schade          : high
                  Denial-of-Service (DoS)
Uitgiftedatum   : 20150120
Toepassing      :
Versie(s)       :
Platform(s)     : Fedora
                  OpenSUSE
                  Ubuntu
Beschikbaarheid : https://kennisbank.ncsc.nl/

Update
   Ubuntu heeft updates beschikbaar gemaakt om de kwetsbaarheid te
   verhelpen. Zie &quot;Mogelijke oplossingen&quot; voor meer informatie.

Samenvatting
   Er is een kwetsbaarheid in libssh ontdekt waarmee een aanvaller een
   Denial-of-Service kan veroorzaken.
```

Figuur 2.2. Koppeling NCSC-adviezen aan CVE-nummers en exploits



De CVE-nummers die in zowel een NCSC-advies als bij een exploit staan gebruiken wij om de twee databases aan elkaar te koppelen.

De dataset met NCSC-adviezen is te verbinden met de tweede database die we gebruiken: dat is een database die gegevens over exploits bevat. De exploits waar we de NCSC-adviezen mee verbinden zijn afkomstig van een gegevensverzameling die beheerd door vulners.com[6] en bevat informatie over exploits uit verschillende andere verzamelingen[7]. Desondanks geeft de door vulners.com beheerde database geen volledig beeld van bestaande exploits, onder andere omdat exploits ook op niet-publieke platformen worden uitgewisseld.

Belangrijk voor ons is dat de verzameldatabase van vulners.com voor exploits de bijbehorende CVE-nummers bevat. Zo kunnen we via de CVE-nummers exploits koppelen aan de bijbehorende NCSC-adviezen. Het koppelproces staat weergegeven in Figuur 2.2 en bestaat uit de volgende stappen:

1. Extractie van alle CVE-nummers die voorkomen in de NCSC-beveiligingsadviezen.
2. Opzoeken van de CVE-nummers in de exploit database. Indien er één of meerdere exploits voor een CVE-nummer beschikbaar zijn noteren we een één. Zijn er geen exploits beschikbaar dan noteren we een nul.
3. Als er een exploit beschikbaar is noteren we de publicatiedatum. Zijn er meerdere exploits die horen bij een CVE-nummer dan kiezen we de publicatiedatum die in de tijd als eerste was.
4. Vervolgens zoeken we per beveiligingsadvies de relevante CVE-nummers op in de door ons gecreëerde tabel. Indien er voor minimaal één CVE-nummer behorende bij het beveiligingsadvies een exploit bekend is noteren we de aanwezigheid van een exploit en de bijbehorende publicatiedatum, namelijk de `Exploit Publicatiedatum' die in de tijd als eerste was.

Dit opzoekproces creëert een tabel zoals hieronder weergegeven.

NCSC-ID	CVE-nummer	Exploit (1=ja, 0=nee)	Exploit Publicatiedatum
NCSC-2012-0001	CVE-2000-0001	1	2000-05-01
NCSC-2012-0002	CVE-2000-0002	0	NA

[6] Zie https://github.com/vulnersCom/getsploit voor openbare pythoncode om de exploit database getsploit gemaakt door vulners.com te benaderen.
[7] Dit zijn de volgende verzamelingen: Immunity Canvas, DSquare Exploit Pack, Exploit-DB, Metasploit, Packet Storm, Malware exploit database, SAINTexploit, seebug.org, Vulnerability Lab, oday.today en Zero Science Lab.

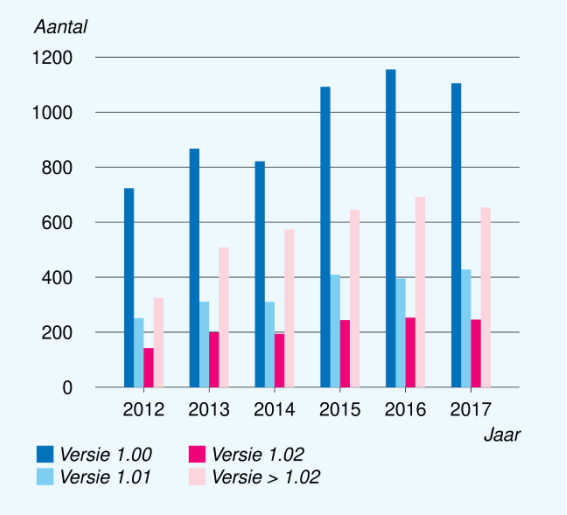
3 Statistieken

In dit hoofdstuk presenteren we door ons geëxtraheerde statistieken. De figuren laten alleen de correlatie tussen verschillende variabelen zien. De onderstaande figuren kunnen niet causaal geïnterpreteerd worden, i.e. oorzaak en gevolg zijn niet af te leiden. Vaak laten we resultaten zien die alleen gaan over versie 1.00 (v1.00) adviezen, dit zijn er 6.515 (uit een totaal van 14.036).

3.1 Verdeling van uitgebrachte adviezen

Om een gevoel te geven voor de hoeveelheid en het type adviezen dat wordt uitgebracht splitsen wij de adviezen naar versienummer en jaar (Figuur 3.1 en Figuur 3.2). Uit Figuur 3.1 valt af te lezen dat er tussen 2012 en 2017 een licht stijgende lijn zit in het aantal nieuw (versie 1.00) uitgebrachte adviezen. De waargenomen stijging kan een reflectie zijn van de toegenomen digitalisering van onze maatschappij, met een daarbij behorende toename in gepubliceerde kwetsbaarheden, of simpelweg een toename van het aantal bij het NCSC geregistreerde systemen[8]. Opvallend is ook dat er relatief veel adviezen met een versienummer groter dan versie 1.02 verschijnen. Desondanks wordt de meerderheid van de adviezen nooit geüpdatet (Figuur 3.2).

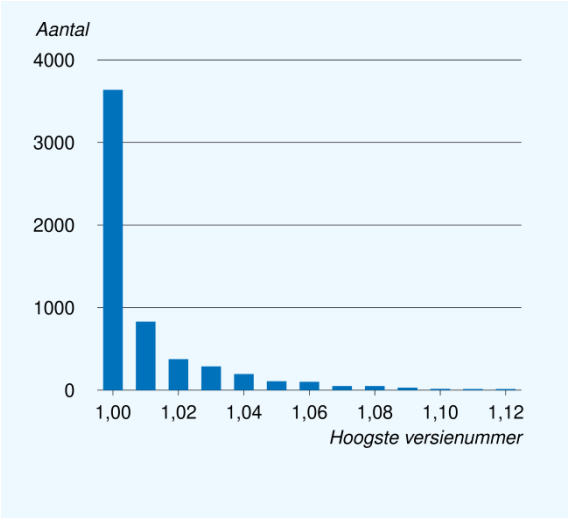
Figuur 3.1. Gepubliceerde adviezen per jaar



NB. Het jaar van publicatie is bepaald op basis van de uitgiftedatum. Merk op dat een advies met versienummer 1.01 of hoger zijn oorsprong moet vinden in een advies met versienummer 1.00 uit hetzelfde of een eerder jaar.

[8] Dit is relevant omdat het NCSC alleen beveiligingsadviezen schrijft over kwetsbaarheden in hard- en software waarvan bekend is dat die gebruikt wordt bij de rijksoverheid of bij vitale processen.

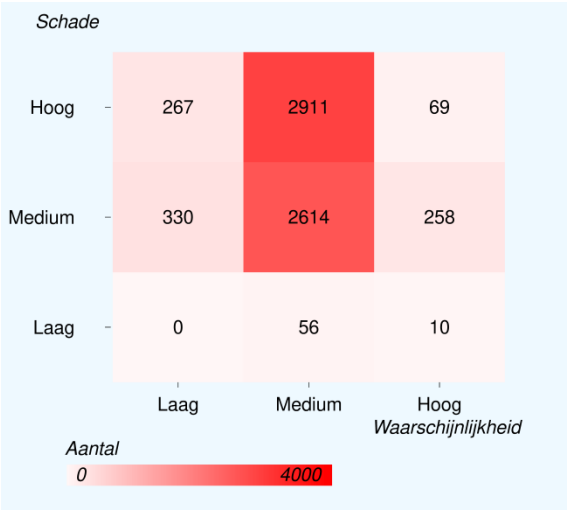
Figuur 3.2. Verdeling adviezen naar hoogst gepubliceerd versienummer



NB. De data in deze grafiek zijn geaggregeerd op advies-ID en bevat de adviezen die tussen 2012-2017 voor het eerst zijn afgegeven – dit zijn er 5.763. Deze data bevatten dus geen v1.01 of hoger adviezen die hun oorsprong vinden in 2011.

3.2 Hoe worden adviezen ingeschaald?

Figuur 3.3. Medium-Hoog adviezen komen het meeste voor

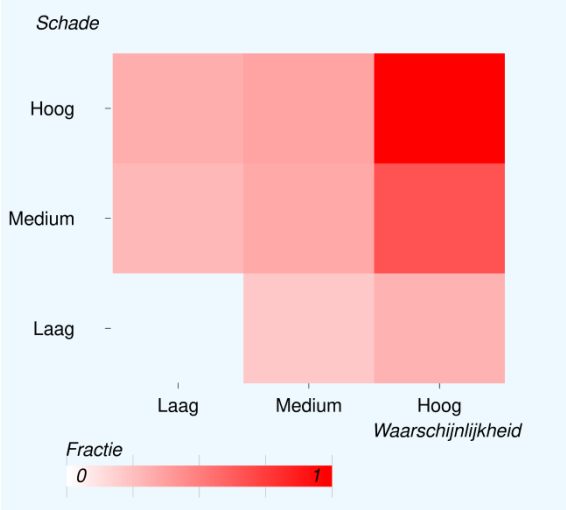


NB. Onderverdeling van NCSC-adviezen naar schade- en waarschijnlijkheidscategorie voor adviezen met versienummer 1.00.

De meeste adviezen die NCSC uitbrengt gaan over kwetsbaarheden die een medium waarschijnlijkheid hebben op misbruik maar die veel schade kunnen veroorzaken. Bijna drieduizend oorspronkelijke (versie 1.00) adviezen worden op die manier geclassificeerd. Figuur 3.3 geeft de mogelijke combinaties van waarschijnlijkheid op misbruik en schade. Op het eerste gezicht valt op dat het aantal laag-laag adviezen gelijk is aan nul. Echter, het is staand beleid om adviezen die in deze categorie vallen niet te publiceren vanwege de beperkte relevantie voor eindgebruikers.

Procentueel krijgen hoog-hoog adviezen het vaakst een update (Figuur 3.4). Bij 99 procent van zulke adviezen komt er een nieuwe versie uit, dat wil zeggen, een update van versie 1.00 naar 1.01. Hier zijn meerdere mogelijke verklaringen voor. Een mogelijke reden is dat NCSC hoog-hoog adviezen beter in de gaten houdt en daardoor vaker stuit op nieuwe – relevante – informatie. Het opduiken van nieuwe informatie zit deels besloten in de reden *waarom* NCSC besluit tot een hoog-hoog advies: het ontbreken van een oplossing, e.g. patch, is een van de drijvers voor het plaatsen in de hoog-hoog categorie. Het verschijnen van bijvoorbeeld een patch wordt daarmee vanzelf relevante informatie die via een update van het originele advies naar de eindgebruikers wordt gecommuniceerd.

Figuur 3.4. Hoog-Hoog adviezen krijgen relatief vaker een update

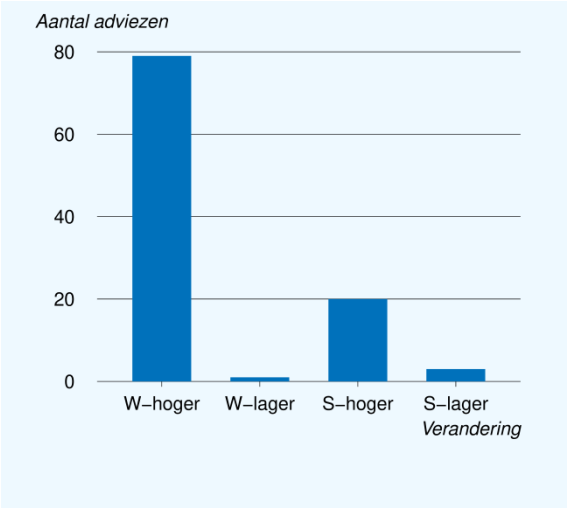


NB. Deze figuur gaat over adviezen die een update krijgen van v1.00 naar v1.01.

Een update gaat vaker gepaard met een verzwaring dan een verlichting van de inschaling voor zowel waarschijnlijkheid als schade (Figuur 3.5). Vooral een verzwaring van de waarschijnlijkheid[9] op misbruik komt relatief vaak voor, terwijl het maar in enkele gevallen voorkomt dat de waarschijnlijkheid van misbruik verlaagd wordt.

[9] In 11 van de gevallen valt de verzwaring samen met een opwaardering van de "wordt de kwetsbaarheid in het wild uitgebuit" inschalingscode. Andere gevallen zijn niet onderzocht.

Figuur 3.5. Adviezen worden bij een update vaker hoger ingeschaald dan lager



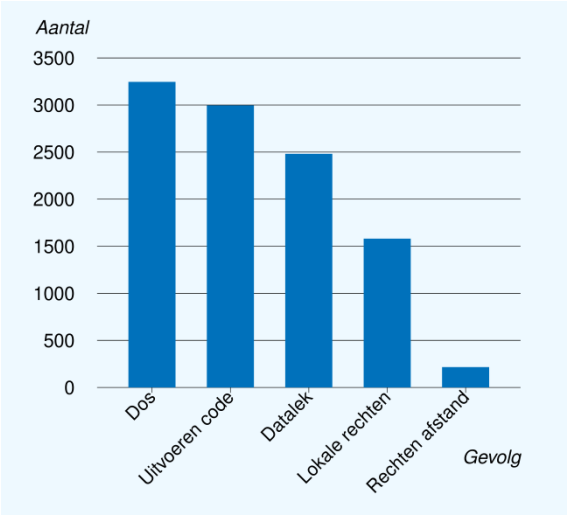
NB. Inschalingsverandering, W staat voor waarschijnlijkheid, S voor schade.

3.3 Welke gevolgen kan een kwetsbaarheid hebben?

Een denial of service (DoS) wordt het meest genoemd als mogelijk gevolg van misbruik van een kwetsbaarheid: bij 3246 adviezen wordt een DoS genoemd als mogelijk gevolg (Figuur 3.6). Op de tweede plek, met 2996 adviezen, vinden we het "uitvoeren van code"[10] door een kwaadwillende en als derde het ontstaan van een datalek. Bekijken we alleen de gevolgen die horen bij adviezen die bij zowel "schade" als "waarschijnlijkheid" als hoog risico worden ingeschaald dan observeren we grofweg hetzelfde beeld. Opvallend is dat "rechten op afstand"[11] relatief vaker voorkomen in hoog-hoog adviezen.

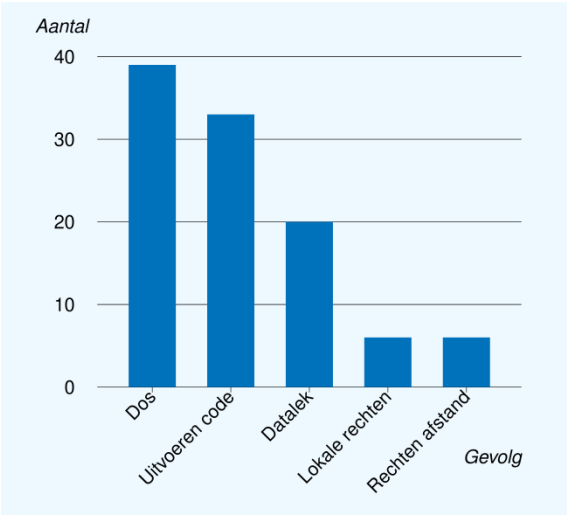
[10] Of, volgens NCSC-documentatie: Na uitbuiting kan code of systeemcommando's worden uitgevoerd.
[11] In de documentatie van NCSC is dit omgeschreven als: Na uitbuiten van de kwetsbaarheid krijgt de aanvaller toegang tot een interactieve (root-)shell op afstand.

Figuur 3.6. Denial of service (DoS) wordt het meest genoemd als potentieel gevolg



NB. Alleen versie 1.00 adviezen zijn meegenomen. In adviezen kunnen meerdere gevolgen genoemd worden. Het totale aantal gevolgen is daarom hoger dan het aantal v1.00 adviezen.

Figuur 3.7. Mogelijke gevolgen voor hoog-hoog adviezen

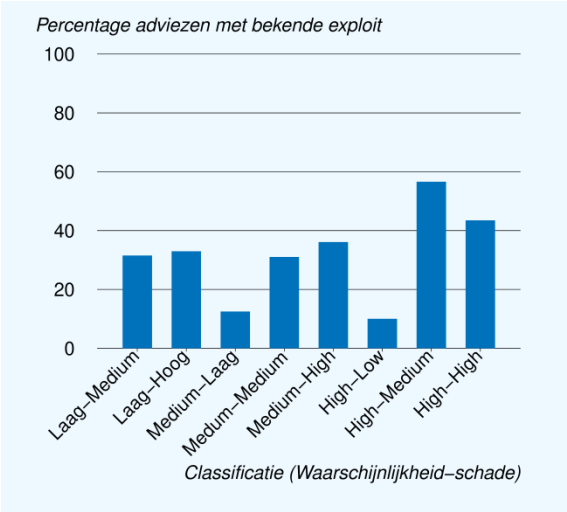


3.4 Over de relatie tussen exploit en advies

De beveiligingsadviezen die NCSC uitbrengt gaan over het bestaan van soft- en hardware kwetsbaarheden. Het bestaan van een kwetsbaarheid betekent niet dat het ook mogelijk is om de kwetsbaarheid uit te buiten. Indien er bijvoorbeeld mitigerende maatregelen zijn genomen kan uitbuiting voorkomen worden. Ook kan het zijn dat er onvoldoende kennis aanwezig is om een kwetsbaarheid uit te buiten. Dat laatste vergt immers de beschikking over exploit code. Hier onderzoeken we voor hoeveel beveiligingsadviezen (en de daarin genoemde kwetsbaarheden) er daadwerkelijk exploitcode beschikbaar is – en of deze informatie betrouwbaar gekoppeld kan worden aan beveiligingsadviezen. We verkrijgen onze gegevens door per beveiligingsadvies te kijken welke CVE-nummers er genoemd worden, en vervolgens in de exploit database op te zoeken of er minstens één exploit bestaat die hoort bij het desbetreffende CVE-nummer.

Wij vinden dat ongeveer dertig procent van alle NCSC-adviezen gekoppeld kan worden aan minstens één exploit uit de vulners.com database (Figuur 3.8). Niet geheel tegen de verwachting observeren we een hoger percentage adviezen met bekende exploits voor de hoog-medium en hoog-hoog categorieën: in deze categorieën wordt de veertig procent zelfs overschreden. Er is hier wel sprake van endogeniteit: wanneer er exploit code beschikbaar is zal aan een beveiligingsadvies sneller een hogere risicocategorie worden toegekend. Merk verder op dat adviezen met een laag-laag categorie nooit worden gepubliceerd waardoor er geen data voor die adviezen beschikbaar zijn.

Figuur 3.8. Voor ongeveer 30 procent van de adviezen bestaat een exploit



NB. Alleen de v1.00 adviezen zijn meegenomen, immers als er een exploit bestaat voor een v1.00 advies, bestaat er ook een exploit voor het v1.01 advies.

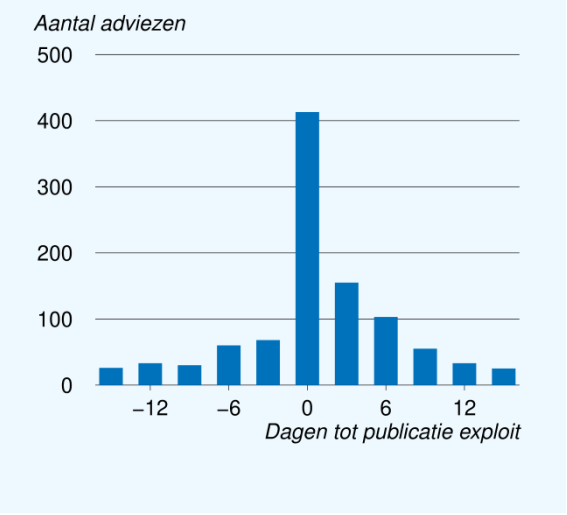
Het is niet alleen interessant om te weten of er exploitcode beschikbaar is, maar ook om te weten *wanneer* die code verschijnt. Immers, indien de exploitcode een significante periode na bekendmaking van een kwetsbaarheid en bijbehorende patch beschikbaar komt, is de kans groot dat de meeste gebruikers weerbaar zijn. Daarom onderzoeken wij hier de tijd tussen de publicatiedatum van een NCSC-advies en de publicatiedatum van een exploit die een kwetsbaarheid misbruikt die in een bepaald advies wordt genoemd. Wij meten deze `tijd tot exploit' (die positief en negatief kan zijn) door te kijken naar het verschil tussen 1) de datum waarop het beveiligingsadvies uitkomt en 2) datum waarop de exploitcode beschikbaar komt in de vulners.com exploit database. Indien de exploit eerder gemeld wordt dan het beveiligingsadvies leidt dit tot negatieve waardes voor `Dagen tot publicatie exploit'.

De data die we verzamelen zijn te zien in Figuur 3.9. In deze figuur zijn de data geclusterd in groepen van drie dagen om rekening te houden met mondiale tijdverschillen. We observeren een sterke piek rondom dag nul. Deze is opvallend maar goed te verklaren. Immers, indien er een exploit is die een bepaalde kwetsbaarheid uitbuit zal er ook een beveiligingsadvies worden uitgebracht. Andersom geldt natuurlijk ook dat indien een kwetsbaarheid bekend wordt deze uitgebuit kan worden door het snel ontwikkelen van exploitcode. Het lijkt misschien vreemd om een beveiligingsadvies uit te brengen zolang er nog geen exploitcode bekend is – immers, waarom zou men slapende honden wakker maken? Er kunnen echter redenen zijn om dit toch te doen. Zo kan er al (een nog onbekende) methode voor uitbuiting bestaan. Verder kan er al een patch beschikbaar zijn en kan men zich dan meteen beschermen tegen de kwetsbaarheid. Het NCSC kiest er dan ook voor om zo snel mogelijk na het bekend worden van een kwetsbaarheid een advies uit te brengen.

Ook kunnen we per jaar bekijken hoeveel adviezen later worden gepubliceerd dan de bijbehorende exploits. Deze uitsplitsing laat zien dat jaarlijks ongeveer 20 procent van de adviezen gelinkt kan worden aan exploits, voorkomend in de vulners.com database, die uitkomen voordat het desbetreffende advies wordt gepubliceerd (Figuur 3.10).

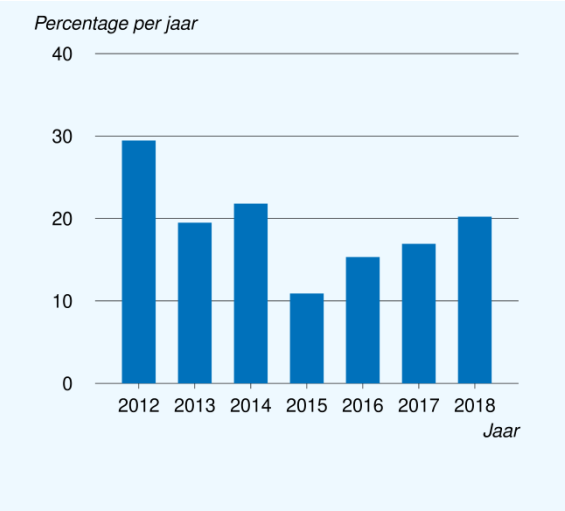
In het vervolg onderzoeken we of de gegevens die we verkrijgen door het koppelen van beveiligingsadviezen aan de exploit database – en dan met name de getallen voor `Dagen tot publicatie exploit' – betrouwbaar zijn.

Figuur 3.9. Veel exploits en adviezen worden rondom dezelfde tijd gepubliceerd



NB. De data zijn weergegeven in bins van drie dagen, e.g. {-1,0,1} is weergegeven als 0 op de horizontale as. In deze figuur zijn alleen v1.00 adviezen meegenomen.

Figuur 3.10. Jaarlijks wordt ongeveer 20 procent van de beveiligingsadviezen later gepubliceerd dan een bijbehorende exploit



NB. Voor v1.00 adviezen die zijn uitgebracht in dat jaar.

We bestuderen de betrouwbaarheid van het datakoppelingsproces door de adviezen die

1. zijn ingeschaald als hoog-hoog, en
2. waarvoor `Dagen tot Publicatie exploit' < 0 geldt

nauwgezet te bestuderen. De twee randvoorwaarden die we gebruiken om een subset aan adviezen te selecteren is zo gekozen dat de voor het NCSC meest relevante beveiligingsadviezen worden geselecteerd: de hoog-hoog adviezen die ogenschijnlijk later zijn gepubliceerd dan exploitcode behorende bij het advies. De zo gemaakte selectie bevat tien adviezen en bijbehorende CVE-nummers, weergegeven in onderstaande tabel:

Tabel 1: Hoog-Hoog adviezen met een negatieve waarde voor de parameter `dagen tot publicatie exploit'.

	CVE-nummer	NCSC-advies
1	CVE-2008-3257	NCSC-2012-0246
2	CVE-2012-2288	NCSC-2012-0639
3	CVE-2013-0156	NCSC-2013-0054
4	CVE-2013-3336	NCSC-2013-0311
5	CVE-2014-2286	NCSC-2014-0184
6	CVE-2014-1300	NCSC-2014-0207
7	CVE-2014-3704	NCSC-2014-0651
8	CVE-2017-5715	NCSC-2018-0009
9	CVE-2015-7501	NCSC-2018-0054
10	CVE-2017-7525	NCSC-2018-0414

Een nadere inspectie van deze adviezen (gedaan met hulp van experts van NCSC) laat het volgende zien:

1. In drie gevallen lijkt er sprake van een *false positive*, i.e., dat vulners.com onterecht melding maakt van een exploit.
2. In één geval is er een fout gemaakt met de invoer van CVE-nummers in het systeem van NCSC.

3. In twee gevallen was het verschil één dag [dagen tot publicatie exploit =-1], wat waarschijnlijk veroorzaakt wordt door het weergeven van tijd in verschillende tijdzones[12].
4. In één geval gaat het om een niet-geverifieerde exploit op Exploit-DB[13].
5. In één geval was er al (vroegtijdig) gewaarschuwd voor een bepaalde softwarekwetsbaarheid (CVE-nummer) in een eerder NCSC-advies met een hoger versienummer dan versienummer 1.00.[14]
6. In één geval meldde een fabrikant van software pas na bekendwording van de exploit dat de kwetsbare software onderdeel uitmaakte van zijn eigen software . Hierdoor wist het NCSC niet dat de betreffende software van een beveiligingsadvies voorzien moest worden. Dit resulteert in een advies dat later gepubliceerd wordt dan de relevante exploitcode.

Gegeven de analyse concluderen we dat alleen voor het advies dat valt onder punt zes en één ander beveiligingsadvies[15] daadwerkelijk sprake was van een negatieve tijd-tot-publicatie-exploit. Voor de resterende acht adviezen zijn er vijf niet-legitieme redenen dat de desbetreffende adviezen opkomen in onze analyse.

Al met al zorgt dit ervoor dat we de dataset waarin we de exploits aan adviezen koppelen niet voor de volle honderd procent betrouwbaar is. Als gevolg hiervan is een exacte analyse van de tijd-tot-publicatie-exploit niet mogelijk.

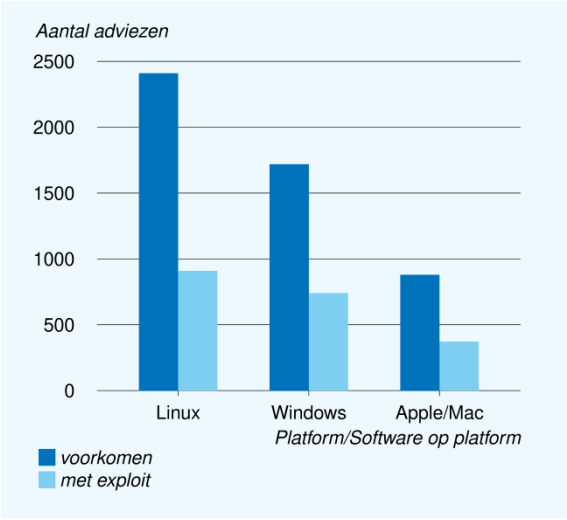
3.5 Onderverdeling adviezen en exploits naar platform

In deze paragraaf onderzoeken we of de aantallen kwetsbaarheden en exploits op verschillende besturingssystemen sterk verschillen. Figuur 3.11 laat zien dat Linux het meest genoemd wordt in de adviezen, vaker dan Windows of Apple. Deze aantallen omvatten naast beveiligingsadviezen voor het besturingssysteem zelf ook adviezen voor software die draait op het besturingssysteem. Daardoor valt er geen conclusie te trekken over de intrinsieke veiligheid van het platform zelf. Dat Linux het meest genoemd wordt kan verklaard worden door het feit dat Linux een populair platform is waar veel doelgroeporganisaties van het NCSC gebruik van maken. In absolute aantallen exploits wordt Linux ook het vaakst vermeld in de vulners.com database.

Relatief gezien is er echter geen platform aan te wijzen dat sterk opvalt: delen we het aantal exploits door het aantal uitgebrachte beveiligingsadviezen dan blijkt voor alle drie de onderzochte platformen voor ongeveer 40 procent van de adviezen ook een exploit voorkomt in de vulners.com database. Indien we wederom uitgaan van een evenredig aantal datafouten per platform, lijkt het dus alsof exploitmakers geen intrinsieke voorkeur voor een bepaald platform lijken te hebben.

[12] Hier houden we rekening mee door data te clusteren in groepen van 3 dagen.
[13] Exploits die door gebruikers worden toegevoegd zijn niet-geverifieerd. Pas na controle op echtheid verandert de status in geverifieerd.
[14] Voor onze analyse hebben we alleen v1.00 adviezen meegenomen, hierdoor vangen we geen meldingen in adviezen met een hoger (dan v1.00) versienummer.
[15] Dit betreft CVE-2008-3257.

Figuur 3.11. Linux wordt het meest genoemd in de beveiligingsadviezen van NCSC



4 Tot slot

Op basis van ons onderzoek concluderen we dat het aantal door NCSC gepubliceerde adviezen in de afgelopen jaren is toegenomen. Dit kan komen door een toename van gerapporteerde kwetsbaarheden, een toename van softwaregebruik bij de doelgroepen van NCSC, of een toename van het aantal doelgroeporganisaties. Van de gepubliceerde adviezen valt slechts een beperkt aantal adviezen (namelijk 69) in de hoogste risicocategorie[16]. Het in de adviezen meest genoemde gevolg bij misbruik van een kwetsbaarheid is een Denial of service.

Wellicht de belangrijkste conclusie van ons onderzoek zijn dat fouten door *false positives*, foutief ingevulde CVE-codes en het bestaan van niet-geverifieerde exploits zorgen voor onbetrouwbare datasets, en dat hierdoor het koppelingsproces niet altijd betrouwbaar is. Vervolgonderzoek dat de relatie tussen beveiligingsadviezen en externe exploit databases onderzoekt is dan ook alleen mogelijk indien er gewerkt kan worden met meer betrouwbare datasets.

[16] Indien we alleen versie 1.00 adviezen meenemen.