Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 17 november 2023

Toegestane verspreiding: TLP:GREEN
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:GREEN en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Welkom bij de End of Week van week 46, 17 november.

Het was weer een drukke week op het gebied van cyber. Veel berichten over crisissen en incidenten in het buitenland, maar gelukkig bleef Nederland grote crisissen bespaard.

We gaan het in deze End of Week hebben over het cyberincident die de havens in Australië plat legde, de Citrix incidenten in het Verenigd Koninkrijk en de aanvallen op de Deense energiesector om af te sluiten met een waarschuwing uit de Verenigde Staten dat aanvallen op de kritieke energie infrastructuur lijken toe te nemen.

Cyber aanval op Australische havens

Australische havens kampte het afgelopen weekend met een cyberincident. Het was hierdoor voor lange tijd niet mogelijk om containers op te halen of af te leveren. Om wat voor soort aanval het precies gaat is nog altijd niet bekendgemaakt. De situatie is inmiddels opgelost zegt DP World, de eigenaar van de haventerminals. De opgelopen achterstand wat betreft het verwerken van containers zal echter nog wel tijd in beslag nemen voordat die weggewerkt is.[1]

Er kwam deze week meer cybernieuws uit Australië. Zo berichtte Australische inlichtingendienst ASD in een nieuw rapport dat twintig procent van de kritieke kwetsbaarheden binnen 48 uur na het verschijnen van een beveiligingsupdate of mitigatie misbruikt wordt.[2]

Citrix-lek zorgde in VK voor dertien 'nationaal aanzienlijke incidenten'

'Een kwetsbaarheid in Citrix NetScaler (CVE-2023-3519) zorgde dit jaar voor dertien 'nationaal aanzienlijke incidenten' in het Verenigd Koninkrijk, zo heeft het Britse National Cyber Security Centre bekendgemaakt. Citrix waarschuwde in juli voor het zerodaylek, dat actief bij aanvallen werd gebruikt, en kwam ook met updates. Het NCSC ontving dit jaar een recordaantal van tweeduizend meldingen over beveiligingsincidenten.'[3]

Grote cyberaanval Denemarken

Volgens een nieuw rapport van SektorCERT, het cybersecuritycentrum voor de Deense vitale sectoren, werd de kritieke infrastructuur van Denemarken dit voorjaar getroffen door de grootste cyberaanval in de geschiedenis van het land. In slechts een paar dagen tijd werden 22 energiebedrijven gehackt. De aanvallen bleven onopgemerkt door gewone Deense burgers, maar verstoorden de bedrijfsvoering aanzienlijk. SektorCERT stelt dat de compromittatie mogelijk was omdat bedrijven hadden nagelaten de updates te installeren.[4]

[1] https://www.abc.net.au/news/2023-11-13/dp-world-deals-with-impact-of-cyber-attack/103097658

[2] https://www.security.nl/posting/818726/

[3] https://www.security.nl/posting/818332/

[4] https://sektorcert.dk/

‘Alarmerende toename van ransomware-operaties gericht op de energiesector’

‘Resecurity, Inc. Een Amerikaans bedrijf dat grote Fortune 100-bedrijven en overheidsinstanties wereldwijd ondersteunt met cybersecurity, heeft een alarmerende toename vastgesteld van ransomware-actoren die zich richten op de energiesector. Het afgelopen jaar hebben ransomware-actoren zich gericht op energie-installaties in Noord-Amerika, Azië en de Europese Unie. In de EU meldde Handelsblatt dat ransomware-aanvallen gericht op de energiesector in 2022 meer dan verdubbeld zijn ten opzichte van het voorgaande jaar.’[5]

[5] https://securityaffairs.com/154113/malware/ransomware-gangs-targets-nuclear-and-oil-gas-2024.html

Beveiligingsadviezen

Zie voor een actueel overzicht: www.ncsc.nl/actueel/beveiligingsadviezen

NCSC-2023-0578 [1.00] [M/H]	Kwetsbaarheden verholpen in Ivanti Secure Access Client
NCSC-2023-0579 [1.00] [L/H]	Kwetsbaarheden verholpen in Ivanti Endpoint Manager Mobile
NCSC-2023-0580 [1.00] [L/H]	Kwetsbaarheid verholpen in Checkpoint Endpoint Security
NCSC-2023-0426 [1.03] [H/H]	Kwetsbaarheden verholpen in Juniper JunOS
NCSC-2023-0581 [1.00] [M/H]	Kwetsbaarheden verholpen in SAP producten
NCSC-2023-0582 [1.00] [M/H]	Kwetsbaarheden verholpen in Siemens producten
NCSC-2023-0583 [1.00] [M/M]	Kwetsbaarheden verholpen in TYPO3 Core
NCSC-2023-0584 [1.00] [M/M]	Kwetsbaarheden verholpen in Microsoft Edge
NCSC-2023-0585 [1.00] [M/H]	Kwetsbaarheden verholpen in Microsoft Exchange Server
NCSC-2023-0586 [1.00] [L/H]	Kwetsbaarheden verholpen in Microsoft Dynamics
NCSC-2023-0587 [1.00] [M/M]	Kwetsbaarheden verholpen in Microsoft Office
NCSC-2023-0588 [1.00] [L/H]	Kwetsbaarheden verholpen in Microsoft System Center
NCSC-2023-0589 [1.00] [M/M]	Kwetsbaarheden verholpen in Microsoft Developer Tools
NCSC-2023-0590 [1.00] [M/H]	Kwetsbaarheden verholpen in Microsoft Azure
NCSC-2023-0591 [1.00] [M/H]	Kwetsbaarheden verholpen in Microsoft Windows
NCSC-2023-0592 [1.00] [M/H]	Kwetsbaarheden verholpen in HPE Aruba Access Points
NCSC-2023-0593 [1.00] [M/H]	Kwetsbaarheid verholpen in VMware Cloud Director Appliance
NCSC-2023-0594 [1.00] [M/M]	Kwetsbaarheden verholpen in Fortinet FortiClient
NCSC-2023-0595 [1.00] [M/H]	Kwetsbaarheden verholpen in Fortinet FortiOS en FortiProxy
NCSC-2023-0596 [1.00] [M/M]	Kwetsbaarheden verholpen in Cisco Identity Services Engine (ISE)

NCSC-2023-0597 [1.00] [M/M]	Kwetsbaarheden verholpen in Adobe After Effects
NCSC-2023-0598 [1.00] [M/M]	Kwetsbaarheden verholpen in Adobe Premiere Pro
NCSC-2023-0599 [1.00] [M/M]	Kwetsbaarheden verholpen in Adobe Audition
NCSC-2023-0600 [1.00] [M/M]	Kwetsbaarheden verholpen in Adobe Media Encoder
NCSC-2023-0601 [1.00] [M/H]	Kwetsbaarheden verholpen in Adobe Dimension
NCSC-2023-0602 [1.00] [M/H]	Kwetsbaarheden verholpen in GIMP
NCSC-2023-0603 [1.00] [M/H]	Kwetsbaarheden verholpen in Fortinet FortiMail
NCSC-2023-0604 [1.00] [M/H]	Kwetsbaarheden verholpen in Adobe Coldfusion
NCSC-2023-0605 [1.00] [M/H]	Kwetsbaarheden verholpen in Adobe Acrobat en Acrobat Reader
NCSC-2023-0606 [1.00] [M/H]	Kwetsbaarheden verholpen in Adobe Photoshop
NCSC-2023-0607 [1.00] [M/M]	Kwetsbaarheid verholpen in Adobe InCopy
NCSC-2023-0608 [1.00] [M/H]	Kwetsbaarheid verholpen in Adobe Animate
NCSC-2023-0609 [1.00] [M/H]	Kwetsbaarheden verholpen in Elastic Kibana en Logstash
NCSC-2023-0610 [1.00] [M/H]	Kwetsbaarheden verholpen in Citrix Hypervisor
NCSC-2023-0611 [1.00] [M/H]	Kwetsbaarheden verholpen in Nagios XI

Wat was er nog meer in het nieuws

FBI: honderden organisaties slachtoffer van Royal-ransomware

'Sinds september vorig jaar zijn honderden organisaties slachtoffer van de Royal-ransomware geworden, waarbij vooral gebruik is gemaakt van phishingmails, zo melden de FBI en het Cybersecurity and Infrastructure Security Agency (CISA) van het Amerikaanse ministerie van Homeland Security.'[6]

FBI haalt IPstorm-botnet offline dat besmette systemen als proxy gebruikte

'De FBI heeft het IPstorm-botnet offline gehaald, dat besmette systemen als proxy gebruikte. Volgens de beheerder, die inmiddels in de Verenigde Staten schuld heeft bekend, telde het botnet 23.000 proxies.'[7]

Cisco: adblockers belangrijke beveiligingsmaatregel voor internetgebruikers

'Adblockers zijn een belangrijke maatregel waarmee internetgebruikers zich tegen malafide advertenties, besmette downloads en scams kunnen beschermen, en het is dan ook duidelijk waarom iedereen er één zou moeten gebruiken, zo stelt Jonathan Munshaw van Cisco.'[8]

Google: overheidsinstanties aangevallen via zerodaylek in Zimbra

'Overheidsinstanties in Griekenland, Tunesië, Moldavië, Vietnam en Pakistan zijn eerder dit jaar aangevallen via een zerodaylek in Zimbra, zo meldt Google.'[9]

MySQL servers targeted by 'Ddostf' DDoS-as-a-Service botnet

MySQL-servers zijn het doelwit van het 'Ddostf'-malware. Het doel is om ze onderdeel te maken van een botnet wat vervolgens wordt verhuurd door cybercriminelen.[10]

---

[6] https://www.security.nl/posting/818288/FBI%3A+honderden+organisaties+slachtoffer+van+Royal-ransomware

[7] https://www.security.nl/posting/818448/FBI+haalt+IPstorm-botnet+offline+dat+besmette+systemen+als+proxy+gebruikte

[8] https://www.security.nl/posting/818698/Cisco%3A+adblockers+belangrijke+beveiligingsmaatregel+voor+internetgebruikers

[9] https://www.security.nl/posting/818676/Google%3A+overheidsinstanties+aangevallen+via+zerodaylek+in+Zimbra

[10] https://www.bleepingcomputer.com/news/security/mysql-servers-targeted-by-ddostf-ddos-as-a-service-botnet/

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

november ’23

TLP:GREEN