Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 5 januari 2024

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

Namens het NCSC wensen we jullie allemaal een Gelukkig Nieuwjaar!

Voor je ligt de End Of Week van 5 januari. Hierin wil ik het graag met jullie hebben over SSH-servers die kwetsbaar zijn voor de Terrapin-aanval, dat de AIVD onderzoek naar statelijke cyberaanvallen gaat intensiveren en dat Tetris voor het eerst in 35 jaar is uitgespeeld.

Aanvullend willen we extra aandacht vragen voor de lijst met gepubliceerde beveiligingsadviezen van deze week en tot slot nog enkele relevante artikelen.

SSH-servers kwetsbaar voor Terrapin-aanval

De Shadowserver Foundation heeft laten weten dat er bijna 11 miljoen SSH-servers wereldwijd kwetsbaar zijn voor de 'Terrapin-aanval'. In Nederland zijn dat er ongeveer 367.000. De Terrapin-kwetsbaarheid (CVE-2023-48795) is vanwege de kwetsbare encryptiemodes lastig te patchen. Om de aanval uit te voeren, moet een aanvaller wel een MitM-positie tussen de client en server hebben waarbij het mogelijk is om verkeer op de TCP/IP-laag te onderscheppen en aan te passen. Daarbij moet voor het opzetten van de verbinding gebruik worden gemaakt van ChaCha20-Poly1305 of de Cipher Block Chaining (CBC) encryptiemode met de optie 'Encrypt-then-MAC'.[1]

AIVD gaat onderzoeken naar statelijke cyberaanvallen intensiveren

Dit jaar zal de AIVD het onderzoek naar cyberaanvallen (uitgevoerd door landen) intensiveren om beter zicht te krijgen op dit soort aanvallen en waar mogelijk om deze aanvallen te mitigeren en andere partijen handelingsperspectief te bieden. Het streven is om nauwer te gaan samenwerken met o.a. het NCSC. Dit wordt genoemd in de jaarplanbrief AIVD 2024, welke naar de Tweede Kamer is gestuurd.[2] [3]

Tetris is uitgespeeld!

Voor het eerst in 35 jaar is Tetris uitgespeeld! De 13-jarige Willis Gibson, een Tetris-fanaat uit de VS, heeft het voor elkaar gekregen. De NES-versie is in 1989 voor het eerst op de markt gekomen en sindsdien zijn er verschillende manier bedacht om de controller sneller te laten bewegen. Hiermee kwam men er na lange tijd achter dat je verder kon komen dan level 29. Willis heeft het record nu op level 157 staan, maar er bestaat zeker een mogelijkheid om dit record nog te verbreken! Wellicht door jou?[4]

[1] https://www.security.nl/posting/824077/Shadowserver%3A+bijna+11+miljoen+SSH-servers+kwetsbaar+voor+Terrapin-aanval

[2] https://www.security.nl/posting/823957/AIVD+gaat+onderzoeken+naar+statelijke+cyberaanvallen+intensiveren

[3] https://open.overheid.nl/documenten/4f81149a-3f31-4ae7-9286-10c8057b68bd/file

[4] https://www.bright.nl/nieuws/1171502/wow-tetris-voor-het-eerst-in-35-jaar-helemaal-uitgespeeld.html

Beveiligingsadviezen

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

NCSC-2023-0654 [1.01][M/H]	Kwetsbaarheden verholpen in OpenSSH
NCSC-2023-0659 [1.00][M/H]	Kwetsbaarheid verholpen in NetApp Active IQ Unified Manager
NCSC-2023-0660 [1.00][M/M]	Kwetsbaarheid verholpen in ProFTPd
NCSC-2023-0661 [1.00][H/M]	Kwetsbaarheden verholpen in Apache OpenOffice
NCSC-2024-0001 [1.00][M/H]	Kwetsbaarheden verholpen in Google Android en Samsung Mobile
NCSC-2024-0002 [1.00][M/H]	Kwetsbaarheden verholpen in Rockwell Automation FactoryTalk Activation Manager

Wat was er nog meer in het nieuws

Niklaus Wirth overleden

Wie kent ze niet: Euler, PL/360, Algol, Pascal, Modula en Oberon. Dit zijn programmeertalen die door Niklaus Wirth zijn uitgebracht. Hij stond er ook om bekend de code zo compact en efficiënt mogelijk te willen schrijven. In 1984 ontving hij een Turing Award.[5] [6]

Kritiek Ivanti-lek

In Ivanti Endpoint Manager zit een kritieke kwetsbaarheid waardoor een aanvaller controle over apparaten kan krijgen. Via een SQL-injection kunnen er, door de aanvaller die toegang tot het netwerk heeft, opdrachten worden uitgevoerd waarmee machines die de Enpoint Manager-agent draaien, zijn over te nemen.[7]

Nieuwe variant van DLL Search Order Hijacking omzeilt Windows 10- en 11-beveiligingen

Een nieuwe variant van DLL Search Order Hijacking maakt gebruik van DLL-bestanden die over het algemeen te vinden zijn in de WinSxS-map. Dit biedt, volgens de onderzoekers, een subtielere en onopvallenderen manier voor DLL Hijacking.[8]

Kwetsbaarheden in Juniper Secure Analytics

Er zijn kwetsbaarheden opgelost in Juniper Secure Analytics. Het gaat hier om alle versies tot en met 7.5.0 UP7. Tot en met vandaag is Juniper SIRT niet op de hoogte van misbruik van deze kwetsbaarheid.[9]

[5] https://tweakers.net/nieuws/217146/pascal-bedenker-en-programmeertaalpionier-niklaus-wirth-is-overleden.html

[6] https://amturing.acm.org/award_winners/wirth_1025774.cfm

[7] https://www.security.nl/posting/824305/Kritiek+Ivanti-lek+kan+aanvaller+controle+over+beheerde+apparaten+geven

[8] https://thehackernews.com/2024/01/new-variant-of-dll-search-order.html

[9] https://supportportal.juniper.net/s/article/2023-12-Security-Bulletin-JSA-Series-Multiple-vulnerabilities-resolved

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

januari ’24

TLP:GREEN