Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 2 februari 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

Welkom bij de End of Week van vrijdag 2 februari.

Op 27 januari alweer 30 jaar geleden kondigde Guido van Rossum versie 1.0.0 van Python aan. [1] Deze week zal ik proberen uw interesse te wekken voor onder meer Ivanti, een ransomware-aanval bij Schneider Electric, een grote hoeveelheid kwetsbare Jenkins Servers en DarkGate-malware

Update Ivanti

In de End of Week van 19 januari vroegen wij al uw aandacht voor de kwetsbaarheden in Ivanti Connect Secure en Policy Secure Gateways. Afgelopen week zijn voor de kwetsbaarheden met kenmerk CVE-2023-46805 en CVE-2024-21887 patches vrijgegeven maar zijn er ook twee nieuwe kwetsbaarheden bekend gemaakt met de kenmerken CVE-2024-21888 en CVE-2024-21893. In een update van het Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) worden federale instanties de opdracht gegeven om Ivanti VPN-apparaten te patchen en tot die tijd los te koppelen. Het NCSC publiceerde en verstuurde hierover ook verschillende berichten. [2] [3]

Schneider Electric getroffen door ransomware-aanval

Volgens een artikel van BleepingComputer heeft Schneider Electric vorige maand te maken gehad met een ransomware-aanval. Een ransomwarebende heeft naar verluidt terabytes aan bedrijfsgegevens gestolen tijdens de cyberaanval en dreigt de gestolen gegevens te lekken als er geen losgeld wordt betaald. Het is niet bekend of Schneider Electric losgeld zal betalen. In een verklaring aan BleepingComputer bevestigde Schneider Electric dat zij te maken kreeg met een cyberaanval en dat de actoren toegang hadden tot gegevens. Het bedrijf zegt echter dat de aanval beperkt was.[4]

Nog 45.000 Jenkins servers kwetsbaar

Het aantal openbare installaties van Jenkins-servers die kwetsbaar zijn voor een onlangs bekendgemaakte kwetsbaarheid loopt in de tienduizenden volgens een scan van shadowserver. Het lijkt erop dat beheerders er niet in slagen de kritieke kwetsbaarheid te patchen waarvan Jenkins heeft gewaarschuwd dat deze zou kunnen leiden tot uitvoering van externe code (RCE).[5]

[1] https://en.wikipedia.org/wiki/History_of_Python

[2] https://www.ncsc.nl/actueel/advisory?id=NCSC-2024-0011

[3] https://www.cisa.gov/news-events/directives/supplemental-direction-v1-ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure

[4] https://www.bleepingcomputer.com/news/security/energy-giant-schneider-electric-hit-by-cactus-ransomware-attack/

[5] https://www.theregister.com/2024/01/30/jenkins_rce_flaw_patch/

DarkGate-malware via Microsoft Teams

Beveiligings-experts van AT&T hebben ontdekt dat Microsoft Teams wordt misbruikt voor phishing en malware-aanvallen. Een klant van AT&T Cybersecurity Managed Detection and Response (MDR) heeft contact opgenomen met zorgen over een gebruiker die zich buiten zijn domein bevond en een ongevraagde Teams-chat naar verschillende interne leden stuurde. Uit een beoordeling van de tactieken en indicatoren van compromissen (IOC's) die door de aanvaller werden gebruikt, bleek dat deze in verband werden gebracht met DarkGate-malware, aldus AT&T.[6]

[6] https://cybersecurity.att.com/blogs/security-essentials/darkgate-malware-delivered-via-microsoft-teams-detection-and-response

Beveiligingsadviezen

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

NCSC-2024-0048 [1.00][M/M]	Kwetsbaarheid verholpen in Progress MOVEit Transfer
NCSC-2024-0011 [1.02][H/H]	Kwetsbaarheden in Ivanti Connect Secure en Policy Secure Gateways
NCSC-2024-0011 [1.03][H/H]	Kwetsbaarheden in Ivanti Connect Secure en Policy Secure Gateways
NCSC-2024-0049 [1.00][M/H]	Kwetsbaarheden verholpen in GNU glibc
NCSC-2024-0050 [1.00][M/H]	Kwetsbaarheid verholpen in Rockwell Automation FactoryTalk
NCSC-2024-0051 [1.00][M/H]	Kwetsbaarheden verholpen in diverse Docker tools

Wat was er nog meer in het nieuws

Politie houdt zes verdachten aan voor phishing en bankhelpdeskfraude

De politie heeft zes mannen aangehouden op verdenking van phishing en bankhelpdeskfraude, waarbij tientallen slachtoffers voor zo'n 70.000 euro werden bestolen. Het lukte de politie ook om live met de verdachten mee te luisteren, die als een 'professioneel belpanel' te werk gingen. [7]

CISA en FBI Secure by Design publicatie

CISA en het Federal Bureau of Investigation (FBI) hebben richtlijnen gepubliceerd over verbeteringen in het beveiligingsontwerp voor fabrikanten van SOHO-apparaten. Meer specifiek vragen de twee bureaus in nieuwe richtlijnen leveranciers om kwetsbaarheden in de webbeheerinterfaces (WMI's) van SOHO-routers te elimineren tijdens de ontwerp- en ontwikkelingsfasen. [8]

Phobos Ransomware-familie breidt uit

Beveiligingsonderzoekers hebben onlangs een nieuwe variant van de beruchte Phobos-ransomwarefamilie ontdekt, genaamd FAUST. Volgens een advies dat vorige week donderdag door FortiGuard Labs werd gepubliceerd, werd de FAUST-variant gevonden in een Office-document dat een VBA-script gebruikte om de ransomware te verspreiden. [9]

NCSC Wall of Fame

Sinds 2022 publiceert het NCSC een jaarlijks terugkerende Wall of Fame om securityonderzoekers met de beste meldingen van het voorgaande jaar in het bijzonder te bedanken. Met het delen van hun kennis over kwetsbaarheden dragen zij direct bij aan een digitaal veilig Nederland. [10]

De verborgen diepten van USB-malware

Een financieel gemotiveerde actor, bekend als UNC4990, maakt gebruik van malafide USB-apparaten om organisaties in Italië aan te vallen. Het is momenteel niet bekend of UNC4990 alleen functioneert als initiële toegangsfacilitator voor andere kwaadwillenden. Het einddoel is vooralsnog niet duidelijk, hoewel in één geval een open-source cryptocurrency-miner zou zijn ingezet. [11]

[7] https://nos.nl/artikel/2506847-zes-aanhoudingen-na-oplichting-met-nephelpdesk-bank-zeker-70-000-euro-weg

[8] https://www.cisa.gov/news-events/alerts/2024/01/31/cisa-and-fbi-release-secure-design-alert-urging-manufacturers-eliminate-defects-soho-routers

[9] https://www.fortinet.com/blog/threat-research/phobos-ransomware-variant-launches-attack-faust

[10] https://www.ncsc.nl/contact/kwetsbaarheid-melden/wall-of-fame

[11] https://www.mandiant.com/resources/blog/unc4990-evolution-usb-malware

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

februari '24

TLP:GREEN