Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 19 april 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

Voor u ligt de End Of Week van 19 april met een selectie van interessante nieuwsberichten van de afgelopen week.

In deze End of Week zal ik proberen uw interesse te wekken voor: een Cyber Security Advisory, een update van ons Palo Alto advisory, een nieuwe LockBit variant, brute-force activiteit en kwetsbaarheden in Ivanti Avalanche.

Gezamenlijke Cyber Security Advisory

Het Federal Bureau of Investigation (FBI) van de Verenigde Staten, de Cybersecurity and Infrastructure Security Agency (CISA), het European Cybercrime Centre (EC3) van Europol en het Nederlandse National Cyber Security Center (NCSC-NL) hebben gezamenlijk een Cyber Security Advisory (CSA) uitgegeven. Sinds 1 januari 2024 heeft de Akira-ransomwaregroep meer dan 250 organisaties getroffen en ongeveer tweeënveertig miljoen (USD) aan ransomware-opbrengsten buit gemaakt. FBI, CISA, EC3 en NCSC-NL moedigen organisaties aan om de aanbevelingen in het hoofdstuk Mitigaties van deze CSA te implementeren om het risico op compromittatie door Akira-ransomware te verkleinen. [1]

Update H/H advies Palo Alto

Vorige week schreven wij over de kwetsbaarheid in PAN-OS 10.2, 11.0 en 11.1 met kenmerk CVE-2024-3400. Inmiddels heeft Palo Alto op hun website aangegeven dat er proof-of-concept door derden openbaar is gemaakt en dat ze bewust zijn van een toenemend aantal aanvallen die misbruik maken van dit beveiligingslek. In eerdere versies van dit advies werd het uitschakelen van Device Telemetry vermeld als een risicobeperkende actie. Het uitschakelen van Device Telemetry is niet langer een effectieve oplossing. Het afgelopen week hebben wij een aantal updates van ons advies uitgebracht. [2] [3]

Nieuwe LockBit variant met zelfverspreidende functies

Cybercriminelen hebben een aangepaste variant van LockBit ingezet die zichzelf kan verspreiden. “De LockBit 3.0-builder is in 2022 gelekt, maar aanvallers gebruiken hem nog steeds actief om aangepaste versies te maken – en er zijn niet eens geavanceerde programmeervaardigheden voor nodig”, aldus Cristian Souza, specialist in incidentrespons bij Kaspersky. Volgens een nieuw rapport van Kaspersky benadrukt het incident ook een zorgwekkende trend waarbij aanvallers geavanceerde ransomware maken

[1] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

[2] https://security.paloaltonetworks.com/CVE-2024-3400

[3] https://advisories.ncsc.nl/advisory?id=NCSC-2024-0170

die zich autonoom binnen netwerken kan verspreiden. [4]

Brute-force-activiteit met veelgebruikte inloggegevens

Cisco waarschuwt voor een grootschalige brute-force-campagne gericht op VPN- en SSH-services op Cisco-, CheckPoint-, Fortinet-, SonicWall- en Ubiquiti-apparaten wereldwijd. Volgens Cisco Talos maakt deze nieuwe brute-force-campagne gebruik van een mix van geldige en generieke gebruikersnamen van werknemers die verband houden met specifieke organisaties. Het Talos-team heeft een volledige lijst met indicatoren van compromissen (IoC's) voor deze activiteit op GitHub gedeeld, inclusief de IP-adressen van de aanvallers voor opname in blokkeerlijsten en de lijst met gebruikersnamen en wachtwoorden die bij de brute-force-aanvallen zijn gebruikt. [5]

Kwetsbaarheden in Avalanche MDM-oplossing

Ivanti heeft beveiligingsupdates uitgebracht om 27 kwetsbaarheden in zijn Avalanche Mobile Device Management (MDM)-oplossing te verhelpen waarvan twee kritiek zijn. De twee kritieke beveiligingsfouten met kenmerk CVE-2024-24996 en CVE-2024-29204 zijn gevonden in de componenten WLInfoRailService en WLAvalancheService van Avalanche. Beide beveiligingsfouten worden veroorzaakt door heap-gebaseerde buffer-overflow-zwakheden, waardoor niet-geverifieerde externe aanvallers willekeurige opdrachten kunnen uitvoeren op kwetsbare systemen met een lage complexiteit en waarvoor geen gebruikersinteractie nodig is. [6]

[4] https://securelist.com/lockbit-3-0-based-custom-targeted-ransomware/112375/

[5] https://blog.talosintelligence.com/large-scale-brute-force-activity-targeting-vpns-ssh-services-with-commonly-used-login-credentials/

[6] https://www.bleepingcomputer.com/news/security/ivanti-warns-of-critical-flaws-in-its-avalanche-mdm-solution/

Beveiligingsadviezen

Zie voor een actueel overzicht: https://advisories.ncsc.nl/advisories

NCSC-2024-0171 [1.00][M/H]	Kwetsbaarheid verholpen in Putty
NCSC-2024-0170 [1.03][H/H]	Kwetsbaarheid verholpen in Palo Alto PAN-OS
NCSC-2024-0172 [1.00][M/H]	Kwetsbaarheden verholpen in IBM Websphere Application Server
NCSC-2024-0173 [1.00][M/H]	Kwetsbaarheden verholpen in Mozilla Firefox, Firefox ESR en Thunderbird
NCSC-2024-0174 [1.00][M/H]	Kwetsbaarheden verholpen in Oracle Communications producten
NCSC-2024-0175 [1.00][M/H]	Kwetsbaarheden verholpen in Oracle Database Producten
NCSC-2024-0176 [1.00][M/H]	Kwetsbaarheden verholpen in Oracle Java SE
NCSC-2024-0177 [1.00][M/H]	Kwetsbaarheden verholpen in Oracle Hyperion
NCSC-2024-0178 [1.00][M/H]	Kwetsbaarheden verholpen in Oracle Analytics
NCSC-2024-0179 [1.00][M/H]	Kwetsbaarheden verholpen in Oracle Fusion Middleware
NCSC-2024-0180 [1.00][M/H]	Kwetsbaarheden verholpen in Oracle Financial Services Applications
NCSC-2024-0181 [1.00][M/H]	Kwetsbaarheden verholpen in Oracle Enterprise Manager
NCSC-2024-0182 [1.00][M/H]	Kwetsbaarheden verholpen in Oracle E-Business Suite
NCSC-2024-0183 [1.00][M/H]	Kwetsbaarheden verholpen in Oracle MySQL
NCSC-2024-0184 [1.00][M/H]	Kwetsbaarheden verholpen in Oracle PeopleSoft
NCSC-2024-0185 [1.00][M/H]	Kwetsbaarheden verholpen in Oracle Supply Chain producten
NCSC-2024-0186 [1.00][M/H]	Kwetsbaarheden verholpen in Oracle Systems
NCSC-2024-0187 [1.00][M/H]	Kwetsbaarheden verholpen in Oracle VirtualBox
NCSC-2024-0188 [1.00][M/H]	Kwetsbaarheden verholpen in Veritas BackupExec

NCSC-2024-0189 [1.00][M/H]	Kwetsbaarheden verholpen in Solarwinds Platform
NCSC-2024-0190 [1.00][M/H]	Kwetsbaarheden verholpen in Owncloud

Wat was er nog meer in het nieuws

Direct hulp bij digitale criminaliteit

Ben je slachtoffer geworden van digitale criminaliteit, zoals phishing of bankhelpdeskfraude, dan moest je voorheen een afspraak maken om aangifte te doen. Dat is vanaf 15 april verleden tijd. Vanaf 15 april komt de politie in Midden-Nederland niet meer alleen voor traditionele criminaliteit, maar ook voor digitale criminaliteit langs bij een slachtoffer. [7]

BabyTV uit aanbod na tweede hack

De zender BabyTV werd 17 april voor de tweede keer overgenomen door kwaadwillenden. BabyTV is een kinderzender die via satelliet wordt verspreid. De zender is recent meerdere malen overgenomen waardoor er over het kanaal Russische propaganda werd uitgezonden. [8]

Tekort aan cyberspecialisten is algemeen probleem

Binnenkort komt demissionair minister Adriaansens van Economische Zaken met een rapport over het tekort aan cybersecurityspecialisten op de arbeidsmarkt. De minister heeft onderzoek laten uitvoeren naar de kwalitatieve en kwantitatieve tekorten op de cybersecurityarbeidsmarkt. De minister merkte verder op dat ze meer vrouwen in de cybersecurity wil zien. [9]

Internationaal phishing-netwerk opgerold

Bij een internationaal samenwerkingsverband van politieorganisaties is een groot phishingnetwerk opgerold. Daarbij zijn in totaal 37 mensen gearresteerd. Vijf van hen werden in Nederland gearresteerd. Het gaat om phishingnetwerk LabHost aldus de Britse politie, die de leiding had over de actie. [10]

Ook jij hebt supply chain risico's

Voor het digitaal veilig functioneren van de Nederlandse samenleving is het belangrijk dat organisaties oog hebben voor risico's in hun supply chain. Dat geldt zeker voor publieke en private organisaties die over zogenoemde Te Beschermen Belangen (TBB) ten aanzien van de Nationale Veiligheid (NV) beschikken. Voor deze organisaties hebben de AIVD, CIO Rijk, het NCSC en de NCTV de Cybercheck ontwikkeld. [11]

[7] https://www.politie.nl/nieuws/2024/april/12/direct-hulp-bij-digitale-criminaliteit.html

[8] https://tweakers.net/nieuws/220968/telenet-en-ziggo-halen-babytv-uit-aanbod-na-tweede-hack-met-russische-propaganda.html

[9] https://www.security.nl/posting/838054/Minister%3A+tekort+aan+cyberspecialisten+op+arbeidsmarkt+algemeen+probleem

[10] https://nos.nl/artikel/2517210-internationaal-phishing-netwerk-opgerold-vijf-arrestaties-in-nederland

[11] https://www.ncsc.nl/actueel/nieuws/2024/april/18/cybercheck-ook-jij-hebt-supply-chain-risicos

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

april ’24

TLP:GREEN