Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 5 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

Dit is de End Of Week van vrijdag 5 april. De Nederlandse ontdekkingsreiziger Jacob Roggeveen ontdekte, op eerste paasdag 5 april in 1722, het zo aan z'n naam gekomen Paaseiland.

In deze End of Week zullen we dieper ingaan op o.a. de XZ utils kwetsbaarheid, een nieuwe DoS aanval en nieuwe ontwikkelingen omtrent kwetsbaarheden in Ivanti. In de media was het echter redelijk rustig deze week. Veel leesplezier gewenst!

Backdoor aangetroffen in XZ Utils

Afgelopen vrijdagavond heeft het NCSC een H/H advies uitgestuurd met betrekking tot XZ Utils met het kenmerk CVE-2024-3094. Een ontwikkelaar heeft een backdoor aangetroffen in recente versies (5.6.0, 5.6.1) van liblzma, een library die wordt meegeleverd als onderdeel van XZ Utils. XZ Utils is een tool die gebruikt wordt voor compressie van data en is in veel Linux distributies aanwezig.

De kwetsbare versies bevatten malafide code, met als einddoel om code te injecteren in de OpenSSH server (SSHD) dat op de machine van het slachtoffer staat. Een aanvaller die in bezit is van een specifieke private key kan willekeurige commando's naar de SSH server versturen. Dit kan leiden tot het uitvoeren van deze commando's met de hoogste rechten.

Op dit moment zijn er geen aanwijzingen dat de backdoor misbruikt is. De backdoor bevindt zich alleen in enkele experimentele distro's en als deze na vrijdagavond nog geüpdatet zijn, is de kans op een malifide versie nog bijzonder klein.[1]

Nieuwe DoS aanval ontdekt

Afgelopen woensdag werd naar buiten gebracht dat kwetsbaarheden in HTTP/2 een denial-of-service (DoS) aanval zou kunnen veroorzaken. De kwetsbaarheid, genaamd de HTTP/2 CONTINUATION Flood, is geïdentificeerd door beveiligingsonderzoeker Bartek Nowotarski. Deze kwetsbaarheid doet zich voor doordat veel HTTP/2-implementaties geen adequate beperkingen opleggen aan het aantal CONTINUATION-frames dat binnen één stream wordt verzonden. Een aanvaller zou de kwetsbaarheid kunnen misbruiken door een aanhoudende stroom van CONTINUATION-frames naar een doelserver te sturen, waardoor de server geheugenfouten kan ervaren en mogelijk crasht. Meerdere producten zouden kwetsbaar zijn, zoals Apache HTTP server (CVE-2024-27316) en Envoy proxy (CVE-2024-27919).[2]

Nieuwe kwetsbaarheden in Ivanti Connect Secure en Policy Secure gateways

Ivanti heeft patches uitgebracht voor nieuwe kwetsbaarheden in Connect Secure en Policy Secure gateways. De kwetsbaarheid met kenmerk CVE-2024-21894 kan misbruikt worden om op afstand willekeurige code uit

[1] https://jfrog.com/blog/xz-backdoor-attack-cve-2024-3094-all-you-need-to-know/

[2] https://www.bleepingcomputer.com/news/security/new-http-2-dos-attack-can-crash-web-servers-with-a-single-connection/

te voeren en zo een denial-of-service aanval mogelijk maakt. Deze kwetsbaarheid wordt veroorzaakt door een heap overflow zwakte in het IPSec component van alle ondersteunde gateway versies.

Ivanti geeft aan dat deze kwetsbaarheid in bepaalde omstandigheden mogelijk zou kunnen leiden tot het uitvoeren van willekeurige code. Dit is echter (nog) niet aangetoond en Ivanti heeft hierover ook geen details vrijgegeven. Wel heeft Ivanti laten weten dat ze geen actief misbruik hebben waargenomen op het moment dat de kwetsbaarheden openbaar werden gemaakt.

Er zijn ook patches uitgebracht voor 3 andere kwetsbaarheden met de kenmerken CVE-2024-22023, CVE-2024-22052 & CVE-2024-22053. Deze zijn voor dezelfde software en zijn te misbruiken door kwaadwillende voor DoS aanvallen.[3] Net NCSC heeft voor deze kwetsbaarheden een advisory uitgebracht met kenmerk NCSC-2024-0144.[4]

[3] https://www.bleepingcomputer.com/news/security/ivanti-fixes-vpn-gateway-vulnerability-allowing-rce-dos-attacks/

[4] https://advisories.ncsc.nl/advisory?id=NCSC-2024-0144

Beveiligingsadviezen

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

NCSC-2024-0140 [v1.00][H/H]	Kwetsbaarheid verholpen in liblzma (XZ Utils)
NCSC-2024-0140 [v1.01][H/H]	Kwetsbaarheid verholpen in liblzma (XZ Utils)
NCSC-2024-0141 [v1.00][M/H]	Kwetsbaarheden verholpen in Google Android en Samsung Mobile
NCSC-2024-0142 [v1.00][L/H]	Kwetsbaarheid verholpen in Flexera Software FlexNet Publisher
NCSC-2024-0143 [v1.00][M/H]	Kwetsbaarheden verholpen in IBM DB2
NCSC-2024-0144 [v1.00][M/H]	Kwetsbaarheden verholpen in Ivanti Connect Secure en Policy Secure Gateways
NCSC-2024-0145 [v1.00][M/H]	Kwetsbaarheid verholpen in Cisco Unified Communications Manager
NCSC-2024-0146 [v1.00][M/H]	Kwetsbaarheden verholpen in Cisco Identity Services Engine
NCSC-2024-0147 [v1.00][M/H]	Kwetsbaarheden verholpen in Cisco Nexus Dashboard
NCSC-2024-0148 [v1.00][M/H]	Kwetsbaarheden verholpen in Lexmark Multifunctionals
NCSC-2024-0149 [v1.00][M/H]	Kwetsbaarheid verholpen in pgAdmin
NCSC-2024-0150 [v1.00][M/M]	Kwetsbaarheid verholpen in IBM Websphere Application Server
NCSC-2024-0151 [v1.00][M/H]	Kwetsbaarheden verholpen in Broadcom Brocade Fabric OS
NCSC-2024-0152 [v1.00][M/H]	Kwetsbaarheden verholpen in Esri Arcgis Portal

Wat was er nog meer in het nieuws

Internetpionier Dan Lynch is overleden op 82-jarige leeftijd

Internetpionier Daniel C. Lynch is zaterdag op 82-jarige leeftijd overleden. Lynch stond bekend om zijn belangrijke rol in de ontwikkeling en wereldwijde adaptatie van tcp/ip-protocollen, die aan de basis staan van het hedendaagse internet.[5]

Amazon’s AI technologie blijkt nog niet geheel zelfstandig

Amazon's "Just walk out" technologie zou er voor moeten zorgen dat klanten niet meer langs traditionele kassa's hoeven door middel van camera's en AI. Echter blijkt uit een rapport van The Information[6] dat ongeveer 700 van iedere 1000 verkopen, handmatig gecheckt moeten worden door Amazon's tech team in India.[7]

Kritieke kwetbaarheid in populaire Wordpress plugin

Voor de Wordpress plugin LayerSlider, een populaire visuele content editor, is een kwetsbaarheid voor SQL injection gevonden. Deze heeft een CVSS score van 9.8, en maakt het mogelijk om gevoelige data, zoals gebruikersinformatie en wachtwoord hashes, uit de gebruikte database te halen. In versie 7.10.1 is deze kwetsbaarheid verholpen.[8]

Google kondigt nieuwe maatregel aan tegen cookiediefstal

Google heeft een nieuwe maatregel aangekondigd die gebruikers tegen cookiediefstal moet beschermen. Het techbedrijf stelt dat het geen nieuwe trackingmethode wordt en gebruikers het kunnen uitschakelen. Volgens Google raken veel internetgebruikers besmet met malware die sessiecookies van het systeem steelt. Deze cookies geven aan dat de gebruiker op een bepaalde website of account is ingelogd. Ze worden aangemaakt nadat de gebruiker is ingelogd.[9]

[5] https://tweakers.net/nieuws/220366/internetpionier-dan-lynch-is-overleden-op-82-jarige-leeftijd.html

[6] https://www.theinformation.com/articles/how-amazons-big-bet-on-just-walk-out-stumbled

[7] https://www.businessinsider.com/amazons-just-walk-out-actually-1-000-people-in-india-2024-4

[8] https://thehackernews.com/2024/04/critical-security-flaw-found-in-popular.html

[9] https://www.security.nl/posting/836476/Google+kondigt+nieuwe+maatregel+aan+tegen+cookiediefstal

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