Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 12 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

Welkom bij de End of Week van vrijdag 12 januari.

De afgelopen week was relatief rustig, dit betekende echter niet dat er niks gebeurde. Zo verscheen woensdag bijvoorbeeld het eerste High/High beveiligingsadvies van 2024! Dit voor kwetsbaarheden in Ivanti Connect Secure en Policy Secure Gateways. Verder kijken we in deze End of Week terug naar 2023 met CVE cijfers en een terugblik van onze Digital Trust Center (DTC) collega's.

2023 CVE Data Review

Security researcher Jerry Gamblin kwam vorige week met een CVE-dataevaluatie en daar komen interessante, onverwachte en voorspelbare dingen uit.

De totale hoeveelheid CVE's nam ook in 2023 weer toe. Er werden in totaal 28.902 CVE's gepubliceerd, dit is 15,23% meer dan in 2022. Sinds 2017 neemt de hoeveelheid CVE's per jaar toe en die trend lijkt zich voort te zetten.

Sommige CVE's worden echter ook weer ingetrokken. Dit jaar werden er 2.112 CVEs gepubliceerd en vervolgens afgewezen.[1]

Gemiddeld werden er 79.18 CVE's per dag gepubliceerd. 22,3% van alle CVE's werd gepubliceerd op een dinsdag, maar dat is met maandelijkse publicatie momenten als Patch-Tuesday niet onverwacht.

De gemiddelde CVSS score was vorig jaar 7.12. Van de hoogste score (10.0) zijn er 36 verschenen. De CVE met de laagste score was CVE-2023-21928 met een score van 1.8.[2]

CVE's kunnen worden uitgegeven door CVE Numbering Authorities (CNAs). CNAs zijn organisaties die zich hebben aangesloten bij het CVE Programma. In Nederland staan 6 CNAs geregisteerd: Airbus, DIVD, Elastic, NLnet Labs, Philips en het NCSC.[3]

DTC Terugblik

Onze Digital Trust Center (DTC) collega's publiceerden vandaag een terugblik op 2023. Het DTC blikt met tevredenheid terug. Er zijn in het 5e jaar dat het DTC bestaat grote stappen gezet om de digitale veiligheid van ondernemend Nederland te vergroten. Zo zijn er in 2023 bijna 140.000 waarschuwingen (notificaties) verstuurd over kwetsbaarheden bij Nederlandse bedrijven. Het bedrijfsleven weet de door het DTC geboden hulpmiddelen steeds beter te vinden; de website is in 2023 ruim 336.000 keer bezocht en de interactieve tools zijn ruim 20.000 keer gebruikt. Lees de volledige terugblik op de website van het DTC.[4]

[1] https://jerrygamblin.com/2024/01/03/2023-cve-data-review/

[2] https://nvd.nist.gov/vuln/detail/CVE-2023-21928

[3] https://www.cve.org/PartnerInformation/ListofPartners

[4] https://www.digitaltrustcenter.nl/nieuws/dtc-blikt-terug-op-2023

Beveiligingsadviezen

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

NCSC-2024-0003 [1.00] [M/H]	Kwetsbaarheden verholpen in IBM DB2
NCSC-2024-0004 [1.00] [M/H]	Kwetsbaarheden verholpen in SAP producten
NCSC-2024-0005 [1.00] [M/H]	Kwetsbaarheden verholpen in Siemens producten
NCSC-2024-0006 [1.00] [M/H]	Kwetsbaarheden verholpen in Microsoft Windows
NCSC-2024-0007 [1.00] [M/H]	Kwetsbaarheden verholpen in Microsoft Office en Sharepoint
NCSC-2024-0008 [1.00] [M/H]	Kwetsbaarheden verholpen in Microsoft Azure
NCSC-2024-0009 [1.00] [L/H]	Kwetsbaarheden verholpen in Microsoft Developer Tools
NCSC-2024-0010 [1.00] [L/H]	Kwetsbaarheid verholpen in Microsoft SQL Server
NCSC-2024-0011 [1.00] [H/H]	Kwetsbaarheden in Ivanti Connect Secure en Policy Secure Gateways
NCSC-2024-0012 [1.00] [M/H]	Kwetsbaarheden verholpen in Cacti
NCSC-2024-0013 [1.00] [M/H]	Kwetsbaarheid verholpen in Fortinet FortiOS en FortiProxy
NCSC-2024-0014 [1.00] [M/H]	Kwetsbaarheden verholpen in Trend Micro Apex One
NCSC-2024-0015 [1.00] [M/H]	Kwetsbaarheden verholpen in Cisco producten
NCSC-2024-0016 [1.00] [M/H]	Kwetsbaarheden verholpen in GitLab Enterprise Edition en Community Edition
NCSC-2024-0017 [1.00] [M/H]	Kwetsbaarheden verholpen in Juniper Junos OS en Junos OS Evolved

Wat was er nog meer in het nieuws

BNR: Nederlandse telefoons online stiekem te volgen: 'Extreem veiligheidsrisico'

"Locatiegegevens van Nederlandse mobiele telefoons zijn online gewoon te koop, blijkt uit onderzoek van BNR. Het gaan en staan van veel Nederlanders is hierdoor tegen betaling te volgen. Het aantal slachtoffers loopt mogelijk in de miljoenen."[5]

Sea Turtle Cyberspionage richt zich op Nederlandse IT and Telecom Bedrijven

Telecommunicatie, media, internetproviders (ISP's), informatietechnologie (IT) - serviceproviders en Koerdische websites in Nederland zijn het doelwit van een nieuwe cyberspionage campagne. De partij die achter de aanvallen zou zitten wordt door Hunt & Hackett Sea Turtle genoemd[6]

Decryptor voor Babuk Tortilla ransomware variant gepubliceerd

"In samenwerking met de Nederlandse politie en Avast heeft Cisco Talos een decryptor gepubliceerd voor bestanden van systemen die getroffen zijn door de Babuk-ransomwarevariant, bekend als Tortilla."[7]

150.000 WordPress-sites over te nemen via kritiek lek in populaire SMTP-plug-in

"Zo'n 150.000 WordPress-sites zijn door een kritieke kwetsbaarheid in een populaire SMTP-plug-in op afstand over te nemen. Een beveiligingsupdate is beschikbaar, maar veel websites hebben die nog niet geïnstalleerd."[8]

NCSC-UK publiceert praktische beveiligingsrichtlijnen voor het MKB

"NCSC-UK heeft donderdag een nieuwe gids voor kleine en middelgrote bedrijven (MKB) gepubliceerd, ontworpen om de potentiële impact van cyberaanvallen bij het gebruik van online diensten te helpen verminderen."[9]

Malware gebruikt bij Ivanti Zero-Day-aanvallen laat zien dat hackers zich voorbereiden op de uitrol van patches

"Ivanti zero-day-kwetsbaarheden genaamd ConnectAround kunnen gevolgen hebben voor duizenden systemen en Chinese cyberspionnen bereiden zich voor op het uitbrengen van patches."[10]

---

[5] https://www.bnr.nl/nieuws/technologie/10537256/nederlandse-telefoons-online-stiekem-te-volgen-extreem-veiligheidsrisico

[6] https://thehackernews.com/2024/01/sea-turtle-cyber-espionage-campaign.html

[7] https://blog.talosintelligence.com/decryptor-babuk-tortilla/

[8] https://www.security.nl/posting/825068/150_000+WordPress-sites+over+te+nemen+via+kritiek+lek+in+populaire+SMTP-plug-in

[9] https://www.infosecurity-magazine.com/news/ncsc-practical-security-guidance/

[10] https://www.securityweek.com/malware-used-in-ivanti-zero-day-attacks-shows-hackers-preparing-for-patch-rollout/

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