Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 15 maart 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 15 maart.

Deze week had als belangrijkste moment het high/high beveiligingsadvies die het NCSC heeft gepubliceerd met betrekking tot FortiOS en Fortiproxy. Verder waren er verschillende interessante nieuwsberichten. Waaronder een uitspraak over het gebruik van Microsoft 365, nog een nieuwtje omtrent Fortinet en nieuwe ontwikkelingen rondom Phobos Ransomware.

In ander nieuws heeft de Duitse overheid een advies over browsergebruik gedeeld, gaat de SIDN het gebruik van security.txt stimuleren en is de website van het hackerkamp Why Hackers Yearn 2025 online.

Veel leesplezier!

Gebruik van Microsoft 365 bij Europese Commissie schendt privacywetgeving

De Europese Commissie schendt de privacywetgeving voor EU-instellingen door Microsoft 365 te gebruiken, volgens de Europese privacytoezichthouder EDPS. De EDPS heeft Brussel opgedragen om vanaf 9 december te stoppen met het doorsturen van gegevens naar Microsoft en zijn partners buiten de EU. De privacytoezichthouder heeft ook geëist dat de Europese Commissie ervoor zorgt dat het gebruik van Microsoft 365 voldoet aan de geldende regelgeving, uiterlijk op 9 december. Brussel heeft volgens de EDPS niet genoeg garanties geboden voor de bescherming van persoonlijke gegevens die buiten de EU worden verzonden. Volgens EDPS-voorzitter Wojciech Wiewiorowski is het de verantwoordelijkheid van EU-instellingen om ervoor te zorgen dat de verwerking van persoonlijke gegevens binnen en buiten de EU gepaard gaat met sterke gegevensbeschermingsmaatregelen. Dit is essentieel om de informatie van individuen te beschermen, zoals vastgelegd in Regelgeving (EU) 2018/1725, wanneer gegevens worden verwerkt door of namens een EU-instelling.[1]

FortiClient EMS kwetsbaarheid verholpen

Dinsdag waarschuwde Fortinet dat het een kritieke kwetsbaarheid heeft opgelost in FortiClient EMS. De kwetsbaarheid (CVE-2023-48788) maakt het voor een aanvaller mogelijk om middels een SQL-injectie code uit voeren onder de hoogste rechten

[1] https://www.security.nl/posting/833336/

(SYSTEM).[2] Onderzoekers van Horizon3 melden dat zij volgende week een Proof of Concept (PoC), Indicators of Compromise (IoC) en een diepgaande uitleg zullen publiceren.[3] Tot die tijd raden zij aan om de DNS log te controleren op verdachte verzoeken. Gebruikers van FortiClient EMS 7.2 wordt met klem geadviseerd om te updaten naar versie 7.2.3 of hoger, gebruikers van 7.0 moeten updaten naar 7.11 of hoger.

Publicatie CISA over Phobos ransomware

De Cybersecurity & Infrastructure Security Agency (CISA) heeft in samenwerking met de FBI en het Multi-State Information Sharing and Analysis Center een update gepubliceerd van de werkwijze van de ransomware-as-a-service Phobos.[4] De ransomware, die sinds 2019 actief is[5], is door de jaren heen geëvolueerd in zowel de manier van verspreiding als van werking. Het begon als afsplitsing van de andere ransomwarefamilie Dharma en is inmiddels doorontwikkeld tot zelfstandig fenomeen. Deze update biedt nieuwe IOC's en TTP's waarmee organisaties zichzelf weerbaar kunnen maken tegen de groepering. Updates zijn onder andere: domeinen waarmee de ransomware wordt geassocieerd, shell commands en e-mailadressen. Het volledige advies kan worden gevonden op de website van CISA[6].

[2] https://twitter.com/Horizon3Attack/status/1767965754744312161

[3] https://www.fortiguard.com/psirt/FG-IR-24-007

[4] https://heimdalsecurity.com/blog/phobos-ransomware-iocs/

[5] https://www.malwarebytes.com/blog/news/2019/07/a-deep-dive-into-phobos-ransomware

[6] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060a

Beveiligingsadviezen

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

NCSC-2024-0107 [v1.00][M/H]	Kwetsbaarheid verholpen in pgAdmin
NCSC-2024-0108 [v1.00][M/H]	Kwetsbaarheden verholpen in Siemens producten
NCSC-2024-0111 [v1.00][M/H]	Kwetsbaarheden verholpen in Microsoft Windows
NCSC-2024-0112 [v1.00][M/H]	Kwetsbaarheden verholpen in Microsoft System Center
NCSC-2024-0113 [v1.00][M/H]	Kwetsbaarheden verholpen in Microsoft Developer Tools
NCSC-2024-0114 [v1.00][M/H]	Kwetsbaarheid verholpen in Microsoft Skype
NCSC-2024-0115 [v1.00][M/H]	Kwetsbaarheden verholpen in Microsoft Azure
NCSC-2024-0116 [v1.00][M/H]	Kwetsbaarheden verholpen in Microsoft Office
NCSC-2024-0117 [v1.00][M/H]	Kwetsbaarheid verholpen in Microsoft Exchange
NCSC-2024-0118 [v1.00][M/H]	Kwetsbaarheid verholpen in Microsoft SQL Server
NCSC-2024-0119 [v1.00][M/H]	Kwetsbaarheid verholpen in Microsoft Dynamics
NCSC-2024-0120 [v1.00][H/H]	Kwetsbaarheden verholpen in Fortinet FortiOS en FortiProxy
NCSC-2024-0121 [v1.00][M/M]	Kwetsbaarheden verholpen in Adobe Animate
NCSC-2024-0122 [v1.00][M/M]	Kwetsbaarheden verholpen in Adobe Bridge
NCSC-2024-0123 [v1.00][M/H]	Kwetsbaarheid verholpen in Adobe ColdFusion
NCSC-2024-0124 [v1.00][M/H]	Kwetsbaarheden verholpen in SAP producten
NCSC-2024-0125 [v1.00][M/M]	Kwetsbaarheid verholpen in Schneider Electric EcoStruxure Power Design
NCSC-2024-0126 [v1.00][M/H]	Kwetsbaarheden verholpen in Cisco IOS XR
NCSC-2024-0127 [v1.00][M/H]	Kwetsbaarheid verholpen in JFrog Artifactory
NCSC-2024-0128 [v1.00][M/H]	Kwetsbaarheden verholpen in Fortinet FortiManager, FortiAnalyzer en FortiClient-EMS

Wat was er nog meer in het nieuws

Desktop client Firefox voldoet aan alle veiligheidseisen volgens Duitse overheid

Het Bundesamt für Sicherheit in der Informationstechnik (BSI) van het Duitse ministerie van Binnenlandse Zaken heeft een nieuw advies omtrent de veiligheid van browsers gepubliceerd. Dit advies wordt sinds 2019 elk jaar gepubliceerd. In het advies van dit jaar wordt geconcludeerd dat Firefox de enige browser is die voldoet aan de minimale veiligheidseisen[7].

Het BSI heeft Firefox, Chrome en Edge, gecontroleerd op technische en organisatorische veiligheidseisen[8]. Voorbeelden hiervan zijn: encryptiemogelijkheden, opties omtrent het beheren van browserdata en documentatie. Naast de desktopbrowser is er ook gekeken naar Firefox en Chrome voor Android en Safari voor iOS.

SIDN: Korting op domeinen met security.txt

De Stichting Internet Domeinregistratie Nederland, verantwoordelijk voor het beheren van het .nl domein, gaat korting geven aan registrars op domeinnamen die een bruikbare security.txt hebben.[9] Security.txt is een tekstbestand wat op een website gezet kan worden met onder andere contactgegevens voor het geval er verdachte activiteiten plaatsvinden. Het gebruiken van security.txt wordt door partijen als het Digital Trust Center (DTC), de Vereniging van Registrars (VvR) en het NCSC gestimuleerd.[10]

Dit maakt het namelijk makkelijker om in contact te komen met organisaties als zij mogelijk slachtoffer zijn van een cybersecurity incident. Deze korting is ter ondersteuning van andere initiatieven van de VvR voor de stimulatie van het gebruik van security.txt, waaronder de ontwikkeling van een Wordpress plugin en best practices.[11]

Why Hackers Yearn 2025

De website van het grootste Nederlandse hackerkamp is deze week gelanceerd. "Why Hackers Yearn 2025"[12] is de tiende editie van het kamp dat sinds 1989 vierjarig wordt georganiseerd voor en door vrijwilligers uit en rondom alle facetten van de internationale hackergemeenschap.

Deze keer zal het kamp worden gehouden van 8 tot 12 augustus 2025 in Geestmerambacht.[13] Mocht je je als vrijwilliger (Angel) willen opgeven, dan is de organisatie daar zeker mee geholpen!

[7] https://www.security.nl/posting/833245/

[8] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Webbrowser/Webbrowser_node.html

[9] https://www.security.nl/posting/833917/

[10] https://www.ncsc.nl/documenten/publicaties/2023/maart/2/handreiking-security.txt

[11] https://www.sidn.nl/nieuws-en-blogs/sidn-introduceert-incentive-om-gebruik-van-security-txt-te-stimuleren

[12] https://why2025.org/Welcome

[13] https://www.openstreetmap.org/?mlat=52.6873&mlon=4.7521#map=15/52.6873/4.7521&layers=P

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

maart ’24

TLP:GREEN