Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 8 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 8 maart.

We gaan het in deze End Of Week eerst hebben over de Duitse Webex die gelekt werd, gevolgd door JetBrains TeamCity en tot slot over cloud security mitigatie strategieën.

We wensen u veel leesplezier.

Duits militair overleg afgeluisterd en gepubliceerd

Zaterdag berichtten verschillende media dat een opname van een vertrouwelijk Duits militairoverleg was gelekt door Rusland. Het gaat om delen van een Webex-overleg van 19 februari. De hoogste baas van de luchtmacht, luitenant-generaal Gerhartz, overlegde toen met officieren over de eventuele inzet van Duitse Taurus-kruisraketten in Oekraïne.

Dinsdag gaf de Duitse defensieminister een persconferentie. Er zou geen sprake geweest zijn van een compromitatie in Duitse defensiesystemen maar door het gebruik van een onbeveiligde verbinding was het afluisteren van het Webex-overleg mogelijk. Het gebruik van deze onbeveiligde verbinding betrof volgens de minister een fout van één van de officieren.[1]

JetBrains TeamCity

Maandag waarschuwde JetBrains dat er twee nieuwe kritieke kwetsbaarheden gevonden zijn in TeamCity On-Premises. De kwetsbaarheden (CVE-2024-27198 en CVE-2024-27199) maken het een kwaadwillende op afstand mogelijk de beveiliging te omzeilen en admin-toegang te verkrijgen.

Gebruikers van TeamCity On-Premises wordt met klem geadviseerd om te updaten naar versie 2023.11.4. TeamCity Cloud servers zijn al gepatcht en zijn niet gecompromitteerd volgens JetBrains.[2]

Inmiddels berichten verschillende organisaties dat er grootschalig misbruik van de kwetsbaarheden plaatsvindt. [3]

[1] https://www.security.nl/posting/832452/Duitse+minister%3A+Webex-overleg+militairen+afgeluisterd+via+onbeveiligde+verbinding

[2] https://blog.jetbrains.com/teamcity/2024/03/additional-critical-security-issues-affecting-teamcity-on-premises-cve-2024-27198-and-cve-2024-27199-update-to-2023-11-4-now

[3] https://www.security.nl/posting/832846/Securitybedrijven+melden+grootschalig+misbruik+van+kritiek+TeamCity-lek

NSA publiceerd top tien cloud security mitigatie strategieën

Het Amerikaanse NSA (National Security Agency) heeft in samenwerking met CISA (Cybersecurity and Infrastructure Security Agency) een top tien lijst gepubliceerd van cloud security mitigatie strategieën**.** Het rapport is een verzameling van tien Cybersecurity Information Sheets (CSIs), een format wat door de NSA en CISA vaker gebruikt wordt. Meer en meer organisaties kiezen voor de cloud en dat is ook niet vreemd gezien de (mogelijke) voordelen. Rob Joyce, NSA's Director of Cybersecurity, onderschrijft de voordelen maar waarschuwt ook: 'Cloud kan IT efficiënter en veiliger maken, maar enkel en alleen als het goed is geïmplementeerd'.[4]

Beveiligingsadviezen

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

NCSC-2024-0095 [1.00] [M/H]	Kwetsbaarheden verholpen in IBM MQ
NCSC-2024-0096 [1.00] [L/H]	Kwetsbaarheid verholpen in Mozilla Thunderbird
NCSC-2024-0097 [1.00] [M/H]	Kwetsbaarheden verholpen in Google Android en Samsung Mobile
NCSC-2024-0098 [1.00] [M/H]	Kwetsbaarheden verholpen in VMware producten
NCSC-2024-0099 [1.00] [M/H]	Kwetsbaarheden verholpen in Foxit PDF Reader en PDF Editor
NCSC-2024-0100 [1.00] [M/H]	Kwetsbaarheden verholpen in ArubaOS en Aruba SD-WAN
NCSC-2024-0101 [1.00] [M/H]	Kwetsbaarheden verholpen in Apple iOS en iPadOS
NCSC-2024-0102 [1.00] [M/M]	Kwetsbaarheden verholpen in Zimbra Collaboration
NCSC-2024-0103 [1.00] [M/H]	Kwetsbaarheid verholpen in Cisco Secure Client
NCSC-2024-0104 [1.00] [M/H]	Kwetsbaarheden verholpen in GitLab Enterprise Edition en Community Edition

[4] https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3699169/nsa-releases-top-ten-cloud-security-mitigation-strategies/

Wat was er nog meer in het nieuws

Dragos: OT Cybersecurity, the 2023 year in review

Het cybersecuritybedrijf Dragos publiceerde deze week haar jaarlijkse OT Cybersecurity Review. Een interessant rapport over kwetsbaarheden, dreigingen en trends gerelateerd aan OT-security.[5]

Hackersgroep eist aanval op bierbrouwerij Duvel op

De ransomwaregroep Stormous heeft de verantwoordelijkheid opgeëist voor de cyberaanval op brouwerij Duvel. Direct nadat de aanval werd gedetecteerd is de productie stopgezet maar inmiddels deels weer opgestart. De ransomwaregroep geeft aan de gestolen data binnen enkele weken te publiceren. [6]

Aanvallers kunnen een Tesla ontgrendelen en stelen

Beveiligingsonderzoekers Talal Haj Bakry en Tommy Mysk beschrijven in hun onderzoek hoe ze een Tesla-auto konden openen en vervolgens stelen via een MiTM-phishing-aanval op de accounts van Tesla-gebruikers. Uit het onderzoek blijkt dat het koppelen van de auto aan een nieuwe telefoon niet over de juiste authenticatiebeveiliging beschikt.[7]

Fakext-campagne gericht op Latijns-Amerika

In november 2023 ontdekten beveiligingsonderzoekers van IBM Security Trusteer nieuwe wijdverbreide malware genaamd Fakext die een kwaadaardige Edge-extensie gebruikt om man-in-the-browser- en webinjectie-aanvallen uit te voeren.[8]

SolarWinds Security Event Manager kwetsbaarheid

SolarWinds heeft een ernstige kwetsbaarheid voor het uitvoeren van externe code (RCE) in zijn Security Event Manager (SEM)-oplossing gepatcht. Door deze kwetsbaarheid met kenmerk CVE-2024-0692, kunnen niet-geverifieerde aanvallers de volledige controle over kwetsbare SEM-installaties overnemen, waardoor mogelijk de deur wordt geopend voor aanvallen binnen uw netwerk.[9]

[5] https://www.dragos.com/ot-cybersecurity-year-in-review/

[6] https://www.nu.nl/tweakers/6304412/hackersgroep-zat-achter-aanval-op-belgische-brouwerij-duvel-moortgat.html

[7] https://www.bleepingcomputer.com/news/security/mitm-phishing-attack-can-let-attackers-unlock-and-steal-a-tesla

[8] https://securityintelligence.com/posts/fakext-targeting-latin-american-banks/

[9] https://securityonline.info/cve-2024-0692-solarwinds-security-event-manager-unauthenticated-rce-flaw/

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