Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 9 februari 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 9 februari 2024.

In deze End of Week vertel ik graag iets over een HIGH/HIGH beveiligingsadvies voor FortiOS, COATHANGER, een campagne over 2FA, een kritieke kwetsbaarheid in TeamCity en tot slot een stukje over Volt Typhoon.

H/H FortiOS

Fortinet waarschuwt voor een nieuwe kritieke kwetsbaarheid in FortiOS, waardoor het mogelijk is om kwetsbare firewalls en vpn-systemen zonder authenticatie op afstand over te nemen.[1] De kwetsbaarheid met kenmerk CVE-2024-21762 maakt het uitvoeren van willekeurige code mogelijk. Er is op dit moment nog geen publieke exploitcode beschikbaar. Door de ernst van de kwetsbaarheid, en de verwachting dat op korte termijn exploitcode zal verschijnen waardoor grootschalig misbruik mogelijk gaat worden, heeft het NCSC een beveiligingsadvies uitgebracht en ingeschaald op HIGH/HIGH.[2] Indien de inzet van de updates niet onmiddellijk mogelijk is, geeft Fortinet aan dat als workaround het uitschakelen van de SSL-VPN overwogen kan worden.

COATHANGER

In 2023 ontdekte het Ministerie van Defensie dat het via malware door China bespied werd. De aanvallers hebben initiële toegang verworven door het exploiteren van een wat oudere buffer-overflow-kwetsbaarheid in FortiOS SSL-VPN.[3] De MIVD heeft een cybersecurity advisory gepubliceerd die analyse biedt over de werking van de COATHANGER-malware en beschrijft diverse beveiligingsmaatregelen.[4] Daarnaast raadt het NCSC aan om risico's van edge devices te beheersen door regelmatig risicoanalyse uit te voeren, beperk toegang tot het internet, voer regelmatig analyses uit op de logging om afwijkende activiteit te detecteren, installeer de meest recente beveiligingsupdates en vervang hard-en software die niet meer ondersteund wordt door de leverancier. Mocht u sporen van COATHANGER-malware aantreffen dan kunt u contact opnemen met het NCSC.

2FA

De Rijksoverheid heeft afgelopen dinsdag het startsein gegeven voor de campagne "Dubbel beveiligd is dubbel zo veilig".[5] Het doel van de campagne is om Nederlanders te stimuleren om tweestapsverificatie in te schakelen voor e-mail en andere online

[1] https://fortiguard.fortinet.com/psirt/FG-IR-24-015

[2] https://www.ncsc.nl/actueel/advisory?id=NCSC-2024-0058

[3] https://www.ncsc.nl/actueel/advisory?id=NCSC-2022-0763

[4] https://www.ncsc.nl/documenten/publicaties/2024/februari/6/mivd-aivd-advisory-coathanger-tlp-clear

[5] https://www.rijksoverheid.nl/actueel/nieuws/2024/02/06/start-campagne-dubbel-beveiligd-is-dubbel-zo-veilig-moet-nederlanders-stimuleren-om-tweestapsverificatie-in-te-stellen-voor-e-mail-en-andere-accounts

accounts. Vrijwilligers gaan de komende weken bij meerdere scholen langs om het belang van tweefactorauthenticatie onder de aandacht te brengen bij jongeren. Afgelopen dinsdag is ook de 21ste editie van "Safer Internet Day" van start gegaan. Met deze campagne wordt wereldwijd aandacht gevraagd om van het internet een veiligere en betere plek te maken voor iedereen, vooral voor kinderen en jongeren.[6]

TeamCity

In een blogpost heeft JetBrains klanten dringend verzocht hun TeamCity-servers te patchen tegen een kritieke kwetsbaarheid.[7] Het betreft een kwetsbaarheid waardoor een ongeauthenticeerde aanvaller met toegang tot een TeamCity-server de authenticatie kan omzeilen en hiermee de kwetsbare instantie met beheerdersrechten kan overnemen. TeamCity is een platform voor softwareontwikkeling en wordt onder andere gebruikt voor het compileren, builden, testen en uitbrengen van software. TeamCity On-Premises versies 2017.1 tot 2023.11.2 zijn kwetsbaar. Volgens shadowserver zijn er wereldwijd meer dan 2.000 TeamCity-servers die online zijn, hoewel er nog geen manier is om te weten hoeveel er al zijn gepatcht.[8]

Volt Typhoon

CISA, de FBI, NSA en partners van de Five Eyes beschrijven in hun advies van 7 februari 2024 hoe Volt Typhoon, door de Verenigde Staten geattribueerd aan de Chinese staat, persistente toegang verkrijgt en behoudt tot vitale infrastructuur in de Verenigde Staten.[9] Dit advies is een opvolging van een eerder advies uit mei 2023 over hetzelfde onderwerp.[10] Het rapport beschrijft verschillende manieren hoe Volt Typhoon ongezien op de netwerken aanwezig blijft en zich lateraal kan bewegen, bijvoorbeeld door het gebruik van Living-of-the-Land technieken. Het doel van de actor lijkt het innemen en behouden van strategische posities op IT-systemen die ook verbonden zijn met OT-assets, en daarnaast digitale spionageactiviteiten. Het rapport biedt verschillende manieren om te detecteren op Volt Typhoon activiteit, waarbij exfiltratie van en/ of activiteit rond het “NTDS.dit” bestand van de Domain Controller een sterke indicatie op malafide activiteit betekent. Verder biedt het rapport een aantal Indicators of Compromise.[11]

[6] https://www.saferinternetday.org/in-your-country

[7] https://blog.jetbrains.com/teamcity/2024/02/critical-security-issue-affecting-teamcity-on-premises-cve-2024-23917/

[8] https://dashboard.shadowserver.org/statistics/iot-devices/time-series/?date_range=7&vendor=jetbrains&model=teamcity&group_by=geo&style=stacked

[9] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[10] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

[11] https://www.cisa.gov/news-events/analysis-reports/ar24-038a

Beveiligingsadviezen

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

NCSC-2024-0011 [v1.04][H/H]	Kwetsbaarheden in Ivanti Connect Secure en Policy Secure Gateways
NCSC-2024-0051 [v1.00][M/H]	Kwetsbaarheden verholpen in diverse Docker tools
NCSC-2024-0052 [v1.00][M/H]	Kwetsbaarheden verholpen in QNAP QTS en QTS Hero
NCSC-2024-0053 [v1.00][M/H]	Kwetsbaarheid verholpen in Nagios XI
NCSC-2024-0054 [v1.00][M/H]	Kwetsbaarheden verholpen in SolarWinds Platform
NCSC-2024-0055 [v1.00][M/H]	Kwetsbaarheden verholpen in Google Android en Samsung Mobile
NCSC-2024-0056 [v1.00][M/H]	Kwetsbaarheden verholpen in VMware Aria Operations Networks
NCSC-2024-0057 [v1.00][M/H]	Kwetsbaarheden verholpen in Cisco Expressway
NCSC-2024-0058 [v1.00][H/H]	Kwetsbaarheden verholpen in Fortinet FortiOS

Wat was er nog meer in het nieuws

Toothbrushes

Volgens een Zwitserse lokale krant Aargauer Zeitung zouden hackers miljoenen slimme tandenborstels met malware geïnfecteerd hebben om een enorme cyberaanval op een Zwitsers bedrijf uit te voeren. De op het internet aangesloten tandenborstels werden aan elkaar gekoppeld in iets dat bekend staat als een botnet om een gedistribueerde Denial of Service (DDoS)-aanval uit te voeren. Volgens Fortinet betrof dit een hypothetisch scenario en geen echte aanval. Hoewel dit verhaal niet echt was, onderstreept dit het steeds groter wordende dreigingslandschap nu IoT steeds meer ingebed raakt in ons dagelijks leven.[12]

Palo Alto

Unit 42, de dreigingsinformatie- en responsafdeling van Palo Alto Networks heeft een rapport uitgebracht over het ransomware-landschap en de aanzienlijke transformaties en uitdagingen die het kende in 2023. In het rapport constateert Unit 42 een 49% toename van het aantal slachtoffers gemeld door ransomware-leksites vergeleken met 2022. Volgens Unit 42 waren er in 2023 specifieke kwetsbaarheden zoals SQL-injectie voor MOVEit- en GoAnywhere MFT-services, evenals een toename van het aantal aanvallen gericht op zero-day-kwetsbaarheden.[13]

AnyDesk

De systemen van AnyDesk werden gehackt door kwaadwillenden die erin slaagden de broncode en privé-sleutels te stelen en wisten hiermee toegang te verkrijgen tot de productiesystemen van het bedrijf. Twee dagen na de openbare verklaring van AnyDesk, onthulde cybersecurity bedrijf "Resecurity" dat ruim 18.000 gecompromitteerde AnyDesk-inloggegevens te koop aangeboden werden op zowel het clear als het dark web.[14]

FortiSIEM

Fortinet heeft twee nieuwe kwetsbaarheden CVE-2024-23108 en CVE-2024-23109 toegevoegd aan een reeds bestaande advies van 10 oktober wat verwarring heeft veroorzaakt.[15] De kwetsbaarheden kunnen op afstand worden uitgevoerd door ongeauthenticeerde kwaadwillende, waarbij geen gebruikersinteractie vereist is. Volgens BleepingComputer gaf Fortinet aan dat de twee nieuwe kwetsbaarheden per ongeluk waren vrijgegeven, vanwege een probleem met de API.[16] Echter blijkt dat CVE-2024-23108 en CVE-2024-23109 feitelijk patch-bypasses zijn voor de CVE-2023-34992-

[12] https://www.bleepingcomputer.com/news/security/no-3-million-electric-toothbrushes-were-not-used-in-a-ddos-attack/

[13] https://unit42.paloaltonetworks.com/unit-42-ransomware-leak-site-data-analysis/

[14] https://www.infosecurity-magazine.com/news/anydesk-hit-cyberattack-customer/

[15] https://www.fortiguard.com/psirt/FG-IR-23-130

[16] https://www.bleepingcomputer.com/news/security/fortinet-warns-of-new-fortisiem-rce-bugs-in-confusing-disclosure/

kwetsbaarheid ontdekt door beveiligingsonderzoeker Zach Hanley. Volgens Fortinet worden binnenkort updates uitgebracht voor 7.0.x, 6.7.x, 6.6.x, 6.5.x en 6.4.x, zonder een verwachte datum te specificeren.

BitLocker

Beveiligingsonderzoeker Stacksmashing bracht Microsoft onlangs in verlegenheid door de Bitlocker-codering binnen een minuut te kraken met behulp van een goedkope Raspberry Pi Pico. Volgens de ethische hacker kunnen kwaadwillenden de Bitlocker-encryptie omzeilen door direct toegang te krijgen tot de hardware en via de LPC-bus de encryptiesleutels uit de TPM te filteren.[17]

[17] https://www.tomshardware.com/pc-components/cpus/youtuber-breaks-bitlocker-encryption-in-less-than-43-seconds-with-sub-dollar10-raspberry-pi-pico

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

februari ’24

TLP:GREEN