Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 22 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 22 maart.

In deze End of Week gaan we in op AcidPour – opvolger van de AcidRain wiper, actief misbruikte Fortinet kwetsbaarheden, een nieuw type DoS aanval en een kwetsbaarheid in Ivanti Standalone Sentry.

AcidPour data wiper

Er is een nieuwe variant van de AcidRain wiper malware publiek beschikbaar gemaakt, genaamd AcidPour.

AcidRain wiper is aan het begin van de oorlog tegen Oekraine ingezet om een groot aantal Viasat routers en modems onklaar te maken. Bij de aanval werden ook onder andere 5800 windmolens in Duitsland getroffen.[1] Deze aanval werd door de Five Eyes landen toegeschreven aan een Russische actor.[2]

De nieuwe AcidPour wiper is in staat om ook alle informatie uit RAID arrays en UBI filesystemen verwijderen. Deze wiper is geschikt om tegen meer soorten hardware en besturingssystemen ingezet te worden dan de AcidRain.[3]

PoC verschenen voor twee recente Fortinet kwetsbaarheden

Afgelopen week heeft het NCSC maar liefst twee beveiligingsadviezen geüpdatet voor producten van Fortinet nadat Proof of Concept (PoC) code is verschenen om de kwetsbaarheden te misbruiken.[4]

Het eerste advies betreft een kwetsbaarheid (CVE-2024-21762)[5] in FortiOS die zich bevindt in sslvpnd. Deze stelt een kwaadwillende in staat om zonder authenticatie willekeurige code uit te voeren op afstand, middels speciaal geprepareerde HTTP-requests. Dit advies was reeds ingeschaald op High/High en het beschikbaar komen van de PoC verandert niets aan die inschaling, maar verhoogt wel het risico op actief misbruik en de urgentie om de beschikbare patch te installeren.[6]

Het tweede beveiligingsadvies gaat over FortiClient-EMS en heeft de eerdere inschaling van Medium/High aangepast naar High/High. De kwetsbaarheid (CVE-2023-48788)[7] waarvoor PoC code publiek beschikbaar is gekomen betreft een SQL injectie die tot code executie kan leiden. Fortinet meldt ook al actief misbruik van deze kwetsbaarheid te zien.[8]

Nieuw type DoS aanval

CISPA heeft deze week een paper naar buiten gebracht waarin een nieuw type

[1] https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

[2] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a

[3] https://thehackernews.com/2024/03/suspected-russian-data-wiping-acidpour.html

[4] https://advisories.ncsc.nl/advisories

[5] https://www.fortiguard.com/psirt/FG-IR-24-015

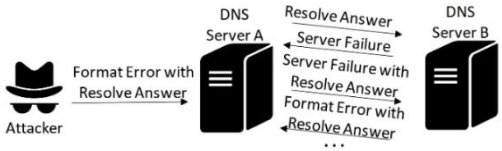
[6] https://advisories.ncsc.nl/advisory?id=NCSC-2024-0058

[7] https://fortiguard.fortinet.com/psirt/FG-IR-24-007

[8] https://advisories.ncsc.nl/advisory?id=NCSC-2024-0128

Denial-of-Service (DoS) aanval wordt beschreven.

Hierbij kan een kwaadwillende, via een gespoofed IP-adres, een data loop veroorzaken tussen twee servers die kwetsbaar zijn voor de aanval. UDP is kwetsbaar voor IP spoofing aangezien het herkomst IP-adressen niet valideert. De aanval wordt geïnitieerd door een foutmelding naar server A met een gespoofed adres van server B te versturen. Hierbij blijven de servers op elkaar reageren met de foutmelding.



Er zijn volgens CISPA 300.000 systemen wereldwijd kwetsbaar voor dit type DoS aanval, waaronder ook systemen van D-Link en TP-Link. De aanvaller zou ook zogenoemde link-flood attacks via de methode zonder eigen botnet op een willekeurig doelwit uit kunnen uitvoeren.

Gebruik van deze aanvalsmethode is nog niet in het wild gezien.[9]

Ivanti Standalone Sentry

Het NATO Cyber Security Centre heeft een kwetsbaarheid gevonden in Ivanti Standalone Sentry. De kwetsbaarheid (CVE-2023-41724)[10] maakt het voor een ongeauthentiseerde aanvaller mogelijk om eenvoudig code uit te voeren op het systeem.

Hiervoor moet de aanvaller wel al toegang hebben tot het lokale netwerk waarop Standalone Sentry draait. Zonder geldig TLS client certificaat is deze kwetsbaarheid niet via het internet uit te buiten en Ivanti heeft geen signalen dat de kwetsbaarheid in de praktijk is misbruikt.[11]

De kwetsbaarheid bevindt zich in alle versies van Standalone Sentry. Het NCSC adviseert om zo snel mogelijk de beschikbare patch te installeren.[12]

[9] https://cispa.de/en/loop-dos

[10] https://forums.ivanti.com/s/article/CVE-2023-41724-Remote-Code-Execution-for-Ivanti-Standalone-Sentry?language=en_US

[11] https://www.bleepingcomputer.com/news/security/ivanti-fixes-critical-standalone-sentry-bug-reported-by-nato/

[12] https://advisories.ncsc.nl/advisory?id=NCSC-2024-0132

Beveiligingsadviezen

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

NCSC-2024-0058 [v1.01][H/H]	Kwetsbaarheden verholpen in Fortinet FortiOS
NCSC-2024-0129 [1.00][M/H]	Kwetsbaarheid verholpen in Autodesk
NCSC-2024-0130 [1.00][M/H]	Kwetsbaarheden verholpen in Mozilla Firefox, Firefox ESR en Thunderbird
NCSC-2024-0131 [1.01][M/H]	Kwetsbaarheden verholpen in Atlassian producten
NCSC-2024-0132 [1.00][M/H]	Kwetsbaarheid verholpen in Ivanti Standalone Sentry
NCSC-2024-0128 [1.01][H/H]	Kwetsbaarheden verholpen in Fortinet FortiManager, FortiAnalyzer en FortiClient-EMS

Wat was er nog meer in het nieuws?

Zorgen over quantumcomputer

Twintig Europarlementariërs hebben in een brief aan de Europese Commissie zorgen geuit over de gevolgen van quantumcomputers voor de beveiliging van gevoelige communicatie. Naar verwachting duurt het nog ruim 10 jaar duurt voordat dit risico zich voor zal doen, maar ook de AIVD benadrukt dat we ons hier zo snel mogelijk op moeten voorbereiden.[13]

Malware aangetroffen op operationele Fujitsu systemen

Fujitsu heeft bekendgemaakt dat op diverse operationele computers van het bedrijf malware is aangetroffen. Het is nog onbekend hoe de malware geplaatst is en of er (gevoelige) informatie is buitgemaakt.[14]

Cyberdreiging voor sectoren lucht- en ruimtevaart neemt toe

Onderzoekers van Resecurity melden een toename aan cyberincidenten te zien gericht op de sectoren lucht- en ruimtevaart. Volgens de directeur cybersecurity van United Airlines brengt het aanwijzen van deze sectoren tot kritieke infrastructuur ook met zich mee dat ze hierdoor een aantrekkelijker doelwit zijn voor actoren die zich voornamelijk op kritieke infrastructuur richten.[15]

Zerodaylekken in Chrome, Edge en Firefox aangetroffen

Een beveiligingsonderzoeker heeft tijdens de Pwn2Own wedstrijd in Vancouver zerodaylekken in diverse browsers gedemonstreerd. De gevolgen van de meeste lekken blijven beperkt tot de browser sandbox. Eén lek in Firefox kan wel misbruikt worden om uit de sandbox uit te breken en het onderliggende systeem te compromitteren.[16]

CISA waarschuwt voor Volt Typhoon

Het Amerikaanse Cybersecurity Infrastructure Security Agency (CISA) heeft een leiders van kritieke infrastructuur gewaarschuwd voor de acute dreiging van Chinese actor Volt Typhoon.[17] In februari had CISA al in samenwerking met de FBI en NSA een advisory over deze actor gepubliceerd.[18]

Iraanse hackers claimen Israelische nucleare faciliteit te hebben gehackt

Een aan Iran gelinkte actor claimt bij een hack op een Israelische nucleare faciliteit duizenden (gevoelige) documenten te hebben buitgemaakt. Het zou onder andere PDF's, e-mails en PowerPoint slides betreffen.[19]

---

[13] https://nos.nl/artikel/2513219-quantumcomputer-gaat-computerbeveiliging-kraken-zorgen-nemen-toe

[14] https://gbhackers.com/fujitsu-hacked/

[15] https://securityaffairs.com/160664/uncategorized/aviation-and-aerospace-sectors-cyber-threats.html

[16] https://www.security.nl/posting/834998/Onderzoeker+toont+zerodaylekken+in+Chrome%2C+Edge%2C+Firefox+en+Safari

[17] https://www.infosecurity-magazine.com/news/cisa-warns-critical-infrastructure/

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

[19] https://news.hitb.org/content/iranian-hackers-claim-have-breached-israeli-nuclear-facility

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