Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 10 november 2023

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

Voor je ligt de End Of Week van 10 november met interessante nieuwsberichten van afgelopen week.

Eerst willen we extra aandacht vragen voor de gepubliceerde presentaties van de One Conference van 3 & 4 oktober jl., de kwetsbaarheid in de SysAid-software en de aangepaste werkwijze voor de Google Chrome beveiligingsadviezen. Aanvullend tref je de lijst met gepubliceerde beveiligingsadviezen van deze week en tot slot nog enkele relevante artikelen.

Presentaties One Conference 2023 online

Op 3 & 4 oktober jl. heb ik weer een onvergetelijke One Conference mogen meemaken. Zoals altijd fijn om het netwerk te begroeten, werkafspraken te maken en sprekers in te leiden bij hun presentaties. Veel van de presentaties zijn opgenomen en nu ook online beschikbaar. Veel kijkplezier! [1]

Kwetsbaarheid in SysAid

Op 8 november is een beveiligingsadvies gepubliceerd over een zeroday-kwetsbaarheid in software van SysAid.[2] Beveiligingsbedrijf Huntress heeft kort daarna een blogpost met aanvullende technische informatie gepubliceerd.[3] De kwetsbaarheid wordt mogelijk misbruikt door DEV-0950 (door sommige beveiligingsbedrijven ook wel Lace Tempest of Cl0p genoemd). In het verleden heeft deze groep diverse zeroday-kwetsbaarheden in filetransfer-applicaties misbruikt.[4] [5] [6] Door misbruik van deze kwetsbaarheden is destijds data geëxfiltreerd die op deze systemen stond opgeslagen. Vervolgens zijn slachtoffers afgeperst waarbij de kwaadwillenden dreigden de data op het internet te publiceren tenzij losgeldbedrag werd betaald. Over de impact van de SysAid-casus is vooralsnog weinig bekend. Waar mogelijk zijn getroffen organisaties, al dan niet via ketenpartners, door het NCSC geïnformeerd.

Google Chrome beveiligingsadviezen

Sinds enige maanden brengt Google wekelijks updates uit voor Google Chrome om sneller kwetsbaarheden te verhelpen. Dit zorgt dus voor een wekelijks beveiligingsadvies van het NCSC, waarin feitelijk de informatie van Google een-op-een wordt overgenomen.

[1] https://emagazine.one-conference.nl/2023/keynotes-and-webinars/

[2] https://www.sysaid.com/blog/service-desk/on-premise-software-security-vulnerability-notification

[3] https://www.huntress.com/blog/critical-vulnerability-sysaid-cve-2023-47246

[4] https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-055a

[5] https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/

[6] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

Ook omdat Google Chrome standaard automatisch updates aanbeveelt en toepast, voegt een wekelijks beveiligingsadvies van het NCSC met daarin de herhaling van Google niets toe. Het NCSC stopt daarom met het schrijven en uitsturen van dit wekelijkse beveiligingsadvies en zal voortaan alleen een beveiligingsadvies voor Google Chrome uitbrengen wanneer het zeer ernstige, of grootschalig misbruikte kwetsbaarheden betreft, waarvoor speciale aandacht nodig is.

Beveiligingsadviezen

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

NCSC-2023-0526 [1.05][H/H]	Kwetsbaarheid verholpen in Cisco IOS XE
NCSC-2023-0562 [1.02][M/H]	Kwetsaarheden verholpen in Qnap QTS en QuTS Hero
NCSC-2023-0570 [1.00][M/H]	Kwetsbaarheid verholpen in Roundcube Webmail
NCSC-2023-0571 [1.00][M/H]	Kwetsbaarheden verholpen in Veeam ONE
NCSC-2023-0572 [1.00][M/H]	Kwetsbaarheden verholpen in Google Android en Samsung Mobile
NCSC-2023-0573 [1.00][M/H]	Kwetsbaarheden verholpen in SolarWinds Platform en Network Configuration Manager
NCSC-2023-0574 [1.00][M/H]	Kwetsbaarheden verholpen in Trend Micro Apex One
NCSC-2023-0575 [1.00][M/M]	Kwetsbaarheid verholpen in Progress WS_FTP
NCSC-2023-0562 [1.03][H/H]	Kwetsbaarheid verholpen in Atlassian Confluence
NCSC-2023-0576 [1.00][M/H]	Kwetsbaarheden verholpen in Foxit PDF Editor
NCSC-2023-0577 [1.00][M/M]	Kwetsbaarheden verholpen in PostgreSQL

Wat was er nog meer in het nieuws

Nordex slachtoffer van fraude

Vorig jaar hebben kwaadwillenden een e-mailaccount van een medewerker geconfisceerd, die werkzaam is bij een fabrikant van zware machines. De kwaadwillenden gebruikten deze toegang om een factuur van in totaal 1,75 miljoen dollar te sturen naar een van de klanten van het bedrijf, windturbinegigant Nordex. Vervolgens is onbewust meer dan 800.000 dollar betaald. Een maand later besefte Nordex dat er sprake was van oplichting en nam contact op met de FBI.[7]

Malvertisingcampagne Windows-nieuwsportaal

In deze nieuwe malvertisingcampagne verspreiden threat actors een gekopieerde versie van een legitiem Windows-nieuwsportaal. Deze wordt vaak bezocht door softwareliefhebbers en systeembeheerders. Zo blijven zij op de hoogte van computerrecensies. Daarnaast gebruiken ze het nieuwsportaal om softwarehulpprogramma's te downloaden.[8]

Sumo Logic security-incident

Van het bedrijf dat zich onder andere richt op logmanagement en SIEM-tools, zijn inloggegevens gestolen. Met deze gegevens heeft een aanvaller zichzelf toegang verleent tot de het AWS-account van Sumo Logic. Mogelijk zijn bij de aanval klantgegevens gestolen; Sumo Logic benadrukt dat het klantgegevens versleuteld opslaat.[9] [10]

Service Location Protocol (SLP) DoS kwetsbaarheid

De Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) waarschuwt voor een kwetsbaarheid in het Service Location Protocol (SLP). Deze bevat een denial-of-service (DoS)-kwetsbaarheid waarbij een niet-geverifieerde, externe aanvaller vervalst UDP-verkeer kan gebruiken om een denial-of-service (DoS)-aanval uit te voeren. [11] [12]

Kwetsbaarheid in Atlassian Confluence

Het NCSC ontvangt meldingen dat kwaadwillenden actief scannen op kwetsbare systemen op het internet en deze aanvallen. De kwaadwillenden resetten/wipen de installatie en nemen deze over middels de weer aanwezige default credentials om vervolgens een extension te installeren die een webshell bevat en zo de Cerber Ransomware uit te rollen. Hoewel de kwetsbaarheid zelf initiële uitvoer van code niet mogelijk maakt is dat via deze deze omweg dus wel mogelijk. [13]

[7] https://www.forbes.com/sites/thomasbrewster/2023/11/07/green-energy-company-fraudsters-sent-50000-to-nigerian-oil-official/

[8] https://cyware.com/news/threat-actors-impersonate-windows-news-portal-to-distribute-redline-stealer-7b320bfd/

[9] https://www.security.nl/posting/817746/Sumo+Logic+waarschuwt+voor+security-incident

[10] https://www.sumologic.com/security-response-center/

[11] https://www.cisa.gov/news-events/alerts/2023/11/08/cisa-adds-one-known-exploited-vulnerability-catalog

[12] https://nvd.nist.gov/vuln/detail/CVE-2023-29552

[13] https://www.ncsc.nl/actueel/advisory?id=NCSC-2023-0562

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

november ’23

TLP:GREEN