Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 10 mei 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 10 mei 2024.

Komende zondag 12 mei is het zeven jaar geleden dat de Wannacry[1] uitbraak heeft plaats gevonden. Deze week waren er gelukkig geen incidenten van dit formaat. Wel was er nieuws over een aanvalsmethode rondom DHCP, de leider van Lockbit en een patch van Citrix. Daarnaast ook nog wat kleine nieuwtjes over Telegram, het Britse ministerie van Defensie, VEEAM, een Australische publicatie en een grootschallige scam campagne.

Deze week verder is er maar een enkel NCSC beveiligingsadvies gepubliceerd over Google Android en Samsung Mobile.

Veel leesplezier!

Tunnelvision: een nieuwe methode om VPN verkeer om te leiden

Onderzoekers van Leviathan Security hebben een manier ontdekt om netwerkverkeer wat bestemd is voor een VPN, om te leiden naar een reguliere netwerk interface[2]. Hiervoor heeft een kwaadwillende toegang nodig tot het netwerk van het slachtoffer en moet in staat zijn om de rol van DHCP-server op zich te nemen, of administrator rechten hebben op de bestaande DHCP-server. Door het gebruik van optie 121 in het DHCP protocol[3] is het mogelijk om de routering tabel van een client aan te passen en hiermee een regel aan te maken die bepaald verkeer over de reguliere interface verstuurd. Dit resulteert erin dat een gebruiker nog denkt dat het verkeer versleuteld is, terwijl een aanvaller in de praktijk mee kan kijken.

Lockbit leaksite opnieuw online, identiteit leider bekend gemaakt

Deze week is de darknet leaksite van Ransomware-as-a-Service groep Lockbit opnieuw online gekomen. De website was in februari van dit jaar offline gehaald en overgenomen door het Britse National Crime Agency (NCA). Toentertijd heeft de NCA in een aantal fases informatie over de groepering op de website gepubliceerd. Deze week hebben ze daar de naam van de leider van de groep aan toegevoegd, Dmitry Yuryevich Khoroshev. Tegelijkertijd met deze openbaring hebben het Verenigd Koninkrijk, de Verenigde Staten en Australië sancties tegen de Russische man aangekondigd. De Verenigde Staten heeft hem daarnaast ook aangeklaagd[4].

[1] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[2] https://www.leviathansecurity.com/blog/tunnelvision

[3] https://datatracker.ietf.org/doc/html/rfc3442

[4] https://www.theregister.com/2024/05/07/alleged_lockbit_kingpin_charged_sanctioned/

Citrix patcht ernstige kwetsbaarheid zonder CVE

Citrix heeft in januari van dit jaar stilletjes een patch uitgebracht voor een ernstige kwetsbaarheid in hun producten Citrix Netscaler ADC en Netscale Gateway. Beveiligingsonderzoekers van Bishopfox hebben toentertijd de kwetsbaarheid gevonden en gemeld bij het bedrijf, deze week hebben de onderzoekers er voor het eerst over gepubliceerd. De kwetsbaarheid stelt een actor in staat om op afstand gevoelige informatie buit te maken doormiddel van een geheugenlek. Het is daarbij erg vergelijkbaar met de Citrix Bleed kwetsbaarheid van vorige jaar[5]. Het grootste verschil is dat de kans dat een actor er zeer gevoelige gegevens mee weet te stelen kleiner is. Citrix heeft alleen geen CVE aan de kwetsbaarheid toegekend, waarbij als reden wordt opgegeven dat het probleem al was verholpen in een nieuwere versie van de software, nog voor het was gemeld bij het softwarebedrijf[6][7]. Speciek is versie 13.1-50.23 kwetsbaar, versies vanaf 13.1-51.15 verhelpen de kwetsbaarheid. De meest recente versie is momenteel 14.1-21.15.

[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4966

[6] https://bishopfox.com/blog/netscaler-adc-and-gateway-advisory

[7] https://www.darkreading.com/cyber-risk/citrix-addresses-high-severity-flaw-in-netscaler-adc-and-gateway?&web_view=true

Beveiligingsadviezen

Zie voor een actueel overzicht: https://advisories.ncsc.nl/advisories

NCSC-2024-0203 [v1.00][M/H]	Kwetsbaarheden verholpen in Google Android en Samsung Mobile

Wat was er nog meer in het nieuws

Telegram onder Belgisch toezicht

De chatapp Telegram zal voortaan bij het Belgisch Instituut voor Post en Telecommunicatie onder toezicht staan. De app, die naast legitiem gebruik ook gebruikt wordt voor criminele zaken als drugshandel of als C2 kanaal voor malware[8], zal door het instituut vervolgd kunnen worden in het geval meldingen, zoals van oproepen tot geweld, niet correct worden afgehandeld[9].

Datalek bij Britse defensie

Er zijn persoonlijke gegevens van Britse defensie medewerkers buitemaakt door een onbekende actor. Het is tot op heden nog niet bekend om hoeveel gegevens het exact gaat. Wel is al bekend dat de hack plaats heeft gevonden via een payrol systeem dat gebruikt wordt door het ministerie. In dit systeem staan onder andere namen en bankgegevens van zowel huidig als oud personeel[10].

VEEAM brengt update uit voor zeer kritieke kwetsbaarheid

VEEAM heeft een kwetsbaarheid voor hun Service Provider Console software gepatcht. De kwetsbaarheid heeft een 9.9 CVSS score en maakt vanwege een onveilige deserialization[11] in een communicatie kanaal het mogelijk voor een actor om arbitraire code uit te voeren op de server waar de software op draait[12].

Richtlijnen voor het kiezen van digitale producten en diensten gepubliceerd

Het Australian Cyber Security Centrum heeft, in samenwerking met hun evenknieën uit Amerika, Canada, het Verenigd Koninkrijk en Nieuw Zeeland, nieuwe aanbevelingen met betrekking tot het kiezen van digitale producenten en diensten die secure-by-design zijn gepubliceerd. De publicatie is er om organisaties te helpen bij het stellen van de juiste vragen tijdens verschillende fases, zoals het aankoopproces, implementatie en end-of-life[13].

Grootschallige scam operatie bloot gelegd

De kranten The Guardian, Die Zeit en Le Monde hebben een onderzoek gepubliceerd waarin een scam campagne met meer dan 70 duizend websites wordt bekend gemaakt. De campagne, die vermoedelijk van Chinese aard is, zou meer dan 800 duizend slachtoffers hebben gemaakt in Europa en Amerika[14].

[8] https://thehackernews.com/2021/04/cybercriminals-using-telegram-messenger.html

[9] https://www.standaard.be/cnt/dmf20240505_96985357

[10] https://www.theregister.com/2024/05/08/uk_opens_investigation_into_contractor/

[11] https://portswigger.net/web-security/deserialization

[12] https://www.veeam.com/kb4575

[13] https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/outsourcing-and-procurement/cyber-supply-chains/choosing-secure-and-verifiable-technologies

[14] https://www.theguardian.com/money/article/2024/may/08/chinese-network-behind-one-of-worlds-largest-online-scams

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

TLP:GREEN