Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 1 december 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

Welkom bij de End of Week van week 48, 1 december 2023.

Om de seizoenen onderling te kunnen vergelijken is voor de meteorologen vandaag de meteorologische winter begonnen.

In deze End of Week zal ik proberen uw interesse te wekken voor een ontmantelde ransomwaregroep, richtlijnen voor veilige AI-systemen, nieuwe zero-day-kwetsbaarheden in IOS en een zero-day-kwetsbaarheid in MagicLine4NX.

Ontmantelde ransomwaregroep

In samenwerking met Europol en Eurojust hebben wetshandhavingsinstanties uit zeven landen leden gearresteerd van een ransomwaregroep Het gaat om een groep die verband houdt met aanvallen op organisaties in 17 landen. De aanvallers verkregen toegang tot de netwerken van hun doelwitten door gebruikersgegevens te stelen, SQL-injectieaanvallen en door phishing-e-mails te gebruiken. Eenmaal binnen gebruikten ze tools als TrickBot-malware, Cobalt Strike en PowerShell Empire om lateraal te bewegen en andere systemen te compromitteren. Deze internationale politieactie werd in september 2019 door de Franse autoriteiten geïnitieerd. [1] [2]

CISA en NCSC-UK onthullen richtlijnen voor veilige AI-systemen

Afgelopen zondag kondigden de Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) en het Britse National Cyber Security Centre (NCSC-UK) de publicatie aan van de Guidelines for Secure AI System Development. De richtlijnen bieden suggesties en oplossingen waarmee datawetenschappers, ontwikkelaars, managers, besluitvormers en risico-eigenaren weloverwogen beslissingen kunnen nemen over het veilige ontwerp, de modelontwikkeling, de systeemontwikkeling, de implementatie en de werking van hun machine learning AI-systemen. CISA nodigt belanghebbenden, partners en het publiek uit om de publicatie te gebruiken om meer te leren over hun strategische visie op AI-technologie en cyberbeveiliging.[3]

Nieuwe Zero-Day-kwetsbaarheden IOS

Apple heeft beveiligingsupdates uitgebracht die twee zero-day-kwetsbaarheden verhelpen voor iPhone-, iPad- en Mac-apparaten. Beide kwetsbaarheden worden actief misbruikt en bevinden zich in de WebKit-browserengine.

[1] https://www.bleepingcomputer.com/news/security/police-dismantle-ransomware-group-behind-attacks-in-71-countries/

[2] https://www.eurojust.europa.eu/news/ransomware-group-dismantled-ukraine-major-operation-supported-eurojust-europol

[3] https://www.cisa.gov/news-events/alerts/2023/11/26/cisa-and-uk-ncsc-unveil-joint-guidelines-secure-ai-system-development

Kwaadwillenden kunnen toegang krijgen tot gevoelige informatie en kunnen willekeurige code uitvoeren op kwetsbare apparaten via kwaadaardige webpagina's. Apple geeft aan dat het op de hoogte is van een rapport dat dit probleem mogelijk is misbruikt in versies van iOS vóór iOS 16.7.1.[4]

Aan Noord-Korea gelinkte APT gebruikt MagicLine4NX zero-day.

Het Britse National Cyber Security Center (NCSC) en de Koreaanse Nationale Inlichtingendienst (NIS) hebben een gezamenlijke waarschuwing uitgegeven dat de aan Noord-Korea gelinkte hackgroep Lazarus een zero-day kwetsbaarheid in de MagicLine4NX-software misbruikt om supply chain-aanvallen uit te voeren. MagicLine4NX is een gezamenlijk certificaatprogramma ontwikkeld door Dream Security, een Zuid-Koreaans bedrijf. Hiermee kunnen gebruikers inloggen met een gezamenlijk certificaat en transacties digitaal ondertekenen. De kwaadwillenden hebben een website gecompromitteerd en kwaadaardige scripts in een artikel geplaatst. De scripts richten zich alleen op bezoekers met een bepaald IP-bereik. Wanneer een gebruiker die de MagicLine4NX-authenticatiesoftware gebruikt de besmette website bezoekt, wordt de kwaadaardige code uitgevoerd waardoor de aanvallers volledige controle over het systeem krijgen. [5] [6]

[4] https://securityaffairs.com/155026/security/apple-emergency-security-updates-2-zero-day.html

[5] https://cyware.com/news/lazarus-group-exploit-magicline4nx-flaw-to-launch-supply-chain-attacks-11b98153

[6] https://eng.nis.go.kr/ECM/1_3_1_1.do?seq=83&currentPage=1

Beveiligingsadviezen

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

NCSC-2023-0617 [v1.01][M/H]	Kwetsbaarheid verholpen in Solarwinds Platform
NCSC-2023-0618 [v1.00][M/M]	Kwetsbaarheden verholpen in MediaWiki
NCSC-2023-0619 [v1.00][M/H]	Kwetsbaarheid verholpen in Apache ActiveMQ
NCSC-2023-0620 [v1.00][M/H]	Kwetsbaarheden verholpen in MOVEit Transfer
NCSC-2023-0621 [v1.00][M/H]	Kwetsbaarheden verholpen in QlikTech Qlik Sense
NCSC-2023-0622 [v1.00][M/H]	Kwetsbaarheden verholpen in Apple iOS, iPadOS, MacOS en Safari
NCSC-2023-0593 [v1.01][M/H]	Kwetsbaarheid verholpen in VMware Cloud Director Appliance
NCSC-2023-0623 [v1.00][M/H]	Kwetsbaarheden verholpen in Google Chrome
NCSC-2023-0624 [v1.00][M/H]	Kwetsbaarheid verholpen in IBM AIX

Wat was er nog meer in het nieuws

Australië adviseert om kritieke kwetsbaarheden binnen 48 uur te patchen

De Australische overheid adviseert om kritieke kwetsbaarheden binnen 48 uur te patchen of op een andere manier te mitigeren. Volgens de Australische overheidsdienst zijn veruit de meeste cyberaanvallen te voorkomen door het implementeren van acht basale beveiligingsmaatregelen. Het NCSC adviseert ook om basismaatregelen te nemen. [7] [8]

Cybercriminelen aarzelen over het gebruik van generatieve AI

Cybercriminelen zijn tot nu toe terughoudend in het gebruik van generatieve AI om aanvallen uit te voeren, zo blijkt uit nieuw onderzoek van Sophos. Bij het onderzoek van vier prominente darkweb-forums ontdekte het bedrijf dat dreigingsactoren weinig interesse toonden in het gebruik van deze tools, en zelfs hun zorgen uitten over de bredere risico's die ze met zich meebrengen. [9]

Risico- en Crisisbarometer

Volgens het publieksonderzoek van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) maakt bijna de helft van de Nederlanders zich zorgen over cyberdreigingen. Deelnemers werd ook per risico en dreiging gevraagd hoe ze hun kennis inschatten. Zeventien procent geeft aan geen kennis over cyberdreigingen te hebben. Eenenveertig procent van de ondervraagden vindt dat de overheid te weinig doet om cyberdreigingen tegen te gaan. [10] [11]

Criminelen verspreiden ransomware via lek in Qlik Sense

Cactus-ransomware wordt actief verspreid via het cloud analytics- en BI-platform Qlik Sense. Dit hebben de beveiligingsspecialisten van Arctic Wolf Labs onlangs ontdekt. De kwaadwillenden maken misbruik van een combinatie van bekende kwetsbaarheden in het cloudanalyse- en BI-platform om de Cactus-ransomware te verspreiden. [12]

Exploitatie van Unitronics PLC's

De Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) onthulde dat kwaadwillenden zich richten op Unitronics Programmable Logic Controllers (PLC's) die worden gebruikt in de water- en afvalwatersystemen. CISA adviseert om het standaardwachtwoord van Unitronics PLC te wijzigen en te controleren dat het standaardwachtwoord niet in gebruik is.

[7] www.security.nl/posting/819632/Australi%C3%AB+adviseert+om+kritieke+kwetsbaarheden+binnen+48+uur+te+patchen

[8] https://www.ncsc.nl/onderwerpen/basismaatregelen

[9] https://www.infosecurity-magazine.com/news/cyber-criminals-hesitant/

[10] www.security.nl/posting/820002/NCTV%3A+bijna+helft+Nederlanders+maakt+zich+zorgen+over+cyberdreigingen

[11] www.nctv.nl/documenten/rapporten/2023/11/29/risico--en-crisisbarometer---najaar-2023

[12] https://www.techzine.eu/news/security/113805/cactus-ransomware-spread-through-bi-platform-qlik-sense/

Bovendien moeten organisaties de PLC loskoppelen van het open internet. Als toegang op afstand nodig is, implementeer dan een firewall/VPN vóór de PLC om de netwerktoegang tot de externe PLC te controleren. [13]

Bluetoothapparaten kwetsbaar voor nieuwe aanval

Op het gebied van draadloze connectiviteit is Bluetooth een alomtegenwoordige technologie die miljarden apparaten over de hele wereld met elkaar verbindt. Door misbruik te maken van een zwakte in de standaard kan met een man-in-the-middle-aanval de communicatie tussen twee gekoppelde of gekoppelde Bluetooth-apparaten worden onderschept, waarna de versleuteling makkelijk te kraken is. Wanneer de aanvaller een voldoende zwakke encryptiesleutel kan forceren, kan hij of zij kwaadaardige gegevens in realtime decoderen en in de communicatiestroom injecteren. [14]

[13] https://industrialcyber.co/utilities-energy-power-water-waste/cisa-responds-to-active-exploitation-of-unitronics-plcs-in-water-and-wastewater-systems-sector/

[14] https://tweakers.net/nieuws/216132/vrijwel-alle-bluetoothapparaten-kwetsbaar-voor-nieuw-ontdekte-aanval.html

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

december '23

TLP:GREEN