Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 15 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 15 december.

In deze End of Week gaan we het hebben over een interview van het DTC. Gevolgd door nieuws uit het buitenland: een ransomware waarschuwing uit Groot Britannië, een ransomware incident in Duitsland en meer samenwerking tussen CISA en ENISA.

Tot slot staan we nog stil bij het tweejarige jubileum van Log4Shell. Taart! (too soon?)

"Vertrouwelijke gesprekken kun je beter in persoon voeren"

Onze collega's van het Digital Trust Center (DTC) hebben een interview gepubliceerd met Manon den Dunnen. Den Dunnen is Strategisch Specialist Digitaal bij de politie en pleit voor een gedragsverandering om veilig om te gaan met informatie in het licht van nieuwe technologische ontwikkelingen zoals AI.

Generatieve AI is aan een snelle opmars bezig. Dat is handig voor ondernemers, maar ook voor cybercriminelen biedt het kansen. Met de komst van handige apps om teksten te generen, beelden te creëren en stemmen te klonen, moeten ondernemers waakzaam zijn. "Het moet normaal worden om even terug te bellen of een controlevraag te stellen. Of bespreek het in persoon."[1]

Britse overheid gewaarschuwd voor 'catastrofale ransomware-aanval'

Het Joint Committee on the National Security Strategy (JCNSS) van het Britse parlement ziet in ransomware-aanvallen een groot risico voor de Britse overheid. Ransomware moet dan ook hoger op de politieke agenda komen, zo staat in een rapport van het Joint Committee on the National Security Strategy (JCNSS) van het Britse parlement. Volgens de parlementscommissie is er meer politieke aandacht en middelen nodig.[2]

LockBit raakt Duits Energieagentschap

Dat de dreiging van ransomware groot is werd ook deze week weer bewezen toen de LockBit-ransomwaregroep bekend maakte dat ze het Duitse Energieagentschap, dena, hebben weten aan te vallen. De cyberaanval werd bekend gemaakt via een bericht op het dark web-platform van LockBit. Op dit platform maken criminelen geslaagde aanvallen bekend en worden de getroffen organisaties toegevoegd aan een groeiende

[1] https://www.digitaltrustcenter.nl/interview-politie-over-AI

[2] https://www.security.nl/posting/821937/Britse+overheid+gewaarschuwd+voor+%27catastrofale+ransomware-aanval

lijst met slachtoffers. dena bevestigde de cyberaanval, maar gaf geen details.[3]

CISA en ENISA tekenen overeenkomst om de samenwerking te verbeteren

Het Agentschap van de Europese Unie voor Cybersecurity (ENISA) heeft een overeenkomst getekend met het Amerikaanse Cybersecurity en Infrastructure Security Agentschap (CISA) om de samenwerking op het gebied van capaciteitsopbouw, de uitwisseling van best practices, en om het gezamenlijke omgevingsbewustzijn te bevorderen.[4]

Log4j

Het was afgelopen zaterdag het tweejarig jubileum van Log4Shell. Veracode, een security bedrijf, leek dat een goede gelegenheid om de huidige staat van Log4j-kwetsbaarheden te onderzoeken en te beoordelen hoe de geleerde lessen de staat van open-source softwarebeveiliging hebben verbeterd. Om dit te doen analyseerde Veracode gegevens van softwarescans tussen 15 augustus en 15 november 2023.

Over het geheel genomen hebben ze vastgesteld dat meer dan 1 op de 3 (38 procent) van de applicaties momenteel kwetsbare versies van Log4j gebruiken.[5]

Dat daar grote risico's aan hangen werd nog extra onderstreept door het bericht dat de Lazarus Group een nieuwe reeks aanvallen uitvoert en daarbij specifiek de Log4Shell kwetsbaarheid uitbuit.[6]

[3] https://heimdalsecurity.com/blog/lockbit-ransomware-targets-german-energy-agency-dena/

[4] https://securityaffairs.com/155606/security/cisa-enisa-signed-working-arrangement.html

[5] https://www.veracode.com/blog/research/state-log4j-vulnerabilities-how-much-did-log4shell-change

[6] https://www.infosecurity-magazine.com/news/lazarus-group-log4shell-flaw/

Beveiligingsadviezen

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

NCSC-2023-0633 [1.00] [M/H]	Kwetsbaarheden verholpen in Apple MacOS
NCSC-2023-0634 [1.00] [M/H]	Kwetsbaarheden verholpen in Apple iOS en iPadOS
NCSC-2023-0635 [1.00] [M/H]	Kwetsbaarheden verholpen in Siemens producten
NCSC-2023-0636 [1.00] [M/M]	Kwetsbaarheden verholpen in Microsoft Windows
NCSC-2023-0637 [1.00] [M/H]	Kwetsbaarheden verholpen in Microsoft Dynamics
NCSC-2023-0638 [1.00] [M/H]	Kwetsbaarheden verholpen in Microsoft Office
NCSC-2023-0639 [1.00] [M/H]	Kwetsbaarheden verholpen in Microsoft Azure
NCSC-2023-0640 [1.00] [M/H]	Kwetsbaarheden verholpen in SAP
NCSC-2023-0641 [1.00] [M/M]	Kwetsbaarheden verholpen in Adobe After Effects
NCSC-2023-0642 [1.00] [M/H]	Kwetsbaarheden verholpen in Adobe Dimension
NCSC-2023-0643 [1.00] [M/H]	Kwetsbaarheden verholpen in Adobe InDesign
NCSC-2023-0632 [1.01] [M/H]	Kwetsbaarheid verholpen in Apache Struts
NCSC-2023-0644 [1.00] [M/M]	Kwetsbaarheden verholpen in Adobe Illustrator
NCSC-2023-0645 [1.00] [M/H]	Kwetsbaarheden verholpen in Fortinet FortiMail
NCSC-2023-0646 [1.00] [M/H]	Kwetsbaarheden verholpen in Zoom
NCSC-2023-0647 [1.00] [M/H]	Kwetsbaarheden verholpen in Nagios XI
NCSC-2023-0648 [1.00] [M/H]	Kwetsbaarheden verholpen in Adobe Illustrator
NCSC-2023-0649 [1.00] [M/H]	Kwetsbaarheden verholpen in Fortinet FortiSandbox
NCSC-2023-0650 [1.00] [M/H]	Kwetsbaarheden verholpen in Fortinet FortiOS
NCSC-2023-0651 [1.00] [M/H]	Kwetsbaarheden verholpen in GitLab Enterprise Edition en Community Edition

Wat was er nog meer in het nieuws

21 Vulnerabilities Proved to Impact Over 86,000 Sierra AirLink Routers

"Researchers revealed 21 new Sierra vulnerabilities impact more than 86,000 online exposed devices."[7]

50.000 WordPress-sites kwetsbaar voor aanvallen door kritiek lek in plug-in

"Zo'n vijftigduizend WordPress-sites bevatten een kritieke kwetsbaarheid waardoor ongeauthenticeerde aanvallers de websites kunnen overnemen."[8]

Mozilla VPN kwetsbaar

Door verschillende kwetsbaarheden in Mozilla VPN konden aanvallers het ip-adres van gebruikers stelen alsmede de WireGuard-encryptiesleutel gebruikt voor de versleuteling, zo ontdekten onderzoekers van securitybedrijf Cure53 die Mozilla's vpn-dienst onderzochten.[9]

[7] https://heimdalsecurity.com/blog/sierra-vulnerabilities-impact-airlink-routers/

[8] https://www.security.nl/posting/821752/50_000+WordPress-sites+kwetsbaar+voor+aanvallen+door+kritiek+lek+in+plug-in

[9] https://www.security.nl/posting/821221/Mozilla+VPN+kon+WireGuard-encryptiesleutel+en+ip-adres+gebruikers+lekken

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