Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 8 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 8 december.

Het einde van 2023 nadert en daarmee zijn er voor de liefhebber ook dit jaar weer diverse CTF[1] uitdagingen[2] beschikbaar[3].

Na een rustige week zonder H/H beveiligingsadvies gaan we in op de grootste cyberoefening van Nederland en LogoFAIL.

ISIDOOR IV is voorbij

De grootste cyberoefening van Nederland is voorbij! Ruim 120 organisaties uit de publieke en private sector en meer dan 3000 personen deden mee aan de cyberoefening ISIDOOR 2023.[4]

Het waren drie intensieve dagen. Er zijn ontzettend veel dingen goed gegaan en er zijn ook veel verbeterpunten geconstateerd. Het evaluatietraject draait op volle toeren.

ISIDOOR is de nationale crisisoefening waarin een nationale cybercrisis wordt gesimuleerd en de gezamenlijke respons wordt beoefend. Eerdere oefeningen waren onder andere in 2015, 2017 en 2021 (ISIDOOR I, II en III). Meer informatie is te vinden op onze website.[5]

Miljoenen PC's kwetsbaar voor 'LogoFAIL' kwetsbaarheid

Onderzoekers hebben een kwetsbaarheid gevonden die gebruikt kan worden om code uit te voeren in processor firmware en SecureBoot te omzeilen. Om deze kwetsbaarheid te misbruiken is geen fysieke toegang vereist.

De kwetsbaarheid - die op 6 december door de onderzoekers is gepresenteerd op BlackHat in Londen[6] – bevind zich in image-parsing libraries in het bootproces van vrijwel alle apparaten die een x86 of ARM-processor gebruiken.

Wanneer het boot logo is vervangen door een malafide PNG en de PC opnieuw wordt opgestart zal de firmware nog voordat SecureBoot wordt uitgevoerd het malafide bestand parsen en code executie worden verkregen.

De enige manier om de kwetsbaarheid te verhelpen is door firmware te updaten zodra een nieuwe versie beschikbaar is.[7]

[1] https://holidayhackchallenge.com/2023/

[2] https://adventofcode.com/

[3] https://tryhackme.com/room/adventofcyber2023

[4] https://nos.nl/artikel/2500763-zo-oefent-nederland-voor-een-grootschalige-cyberaanval

[5] https://www.ncsc.nl/actueel/nieuws/2023/december/8/isidoor

[6] https://www.blackhat.com/eu-23/briefings/schedule/index.html#logofail-security-implications-of-image-parsing-during-system-boot-35042

[7] https://www.darkreading.com/endpoint-security/critical-logofail-bugs-secure-boot-bypass-millions-pcs

Beveiligingsadviezen

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

NCSC-2023-0625 [1.00][M/H]	Kwetsbaarheden verholpen in GitLab Enterprise Edition en Community Edition
NCSC-2023-0626 [1.00][M/H]	Kwetsbaarheden verholpen in IBM DB2
NCSC-2023-0627 [1.00][M/H]	Kwetsbaarheden verholpen in Zyxel producten
NCSC-2023-0628 [1.00][M/H]	Kwetsbaarheden verholpen in Squid
NCSC-2023-0629 [1.00][M/H]	Kwetsbaarheden verholpen in Google Android en Samsung Mobile
NCSC-2023-0630 [1.00][M/H]	Kwetsbaarheid verholpen in Atlassian Confluence
NCSC-2023-0631 [1.00][M/H]	Kwetsbaarheid verholpen in Atlassian Jira
NCSC-2023-0632 [1.00][M/H]	Kwetsbaarheid verholpen in Apache Struts

Wat was er nog meer in het nieuws

Adobe ColdFusion Flaw Used by Hackers to Access US Govt Servers

Het Amerikaanse CISA (Cybersecurity and Infrastructure Security Agency) waarschuwt voor actief misbruik van een kwetsbaarheid in Adobe ColdFusion.[8] Deze kwetsbaarheid zou tussen juni en juli 2023 in minimaal twee gevallen zijn misbruikt om toegang te krijgen tot servers van de Federal Civilian Executive Branch (FCEB).[9]

Datalekzoekmachine Have I Been Pwned bestaat 10 jaar

Inmiddels bevat deze website e-mail adressen van 12,8 miljard accounts die zijn 'gepwned', afkomstig uit 731 websites en datasets.[10]

'Russische FSB hackte jarenlang Britse politici om geheimen te laten uitlekken'

Volgens de Britse overheid zijn sinds 2015 onder andere Britse politici, universiteiten, journalisten, stichtingen, denktanks doelwit van Russische hackers van de FSB. Het doel zijn zou om democratische processen te ondermijnen.[11]

Twintigduizend Microsoft Exchange-servers op internet zijn end-of-life

Op basis van een scan meldt Shadowserver dat circa twintigduizend Microsoft Exchange-servers een versie draaien die end of life is en geen beveiligingsupdates meer ontvangen.[12] Volgens het overzicht van Shadowserver bevinden 559 van deze servers zich in Nederland.[13]

Russian military hackers target NATO fast reaction corps

Onderzoekers van Palo Alto Networks' Unit geven aan dat ze in circa 20 maanden exploitatie van CVE-2023-23397[14] hebben zien plaatsvinden gericht tegen minstens 30 organisaties in 14 NAVO landen. De aanvallen worden door Palo Alto toegeschreven aan de Russische actor APT28.[15]

Digital Trust Center groeit naar 2550 leden

De DTC Community heeft een mijlpaal bereikt van meer dan 500 leden. Op het DTC Community forum kunnen ondernemers laagdrempelig terecht met cybersecurity vragen.[16]

---

[8] https://nvd.nist.gov/vuln/detail/CVE-2023-26360

[9] https://www.hackread.com/adobe-coldfusion-flaw-hackers-access-us-govt-servers/

[10] https://www.security.nl/posting/820599/Datalekzoekmachine+Have+I+Been+Pwned+bestaat+10+jaar

[11] https://tweakers.net/nieuws/216408/russische-fsb-hackte-jarenlang-britse-politici

[12] https://www.security.nl/posting/820618/Twintigduizend+Microsoft+Exchange-servers+end-of-life

[13] https://dashboard.shadowserver.org/statistics/combined/map/?map_type=std&day=2023-11-25&source=exchange&source=exchange6&tag=eol%2B&geo=all&data_set=count&scale=log

[14] https://nvd.nist.gov/vuln/detail/CVE-2023-23397

[15] https://www.bleepingcomputer.com/news/security/russian-military-hackers-target-nato-fast-reaction-corps/

[16] https://www.computable.nl/artikel/nieuws/security/7582794/250449/digital-trust-center-groeit-naar-2550-leden.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