Mesačný prehľad kritických zraniteľností august 2022

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci august 13 kritických a 50 vysoko závažných zraniteľností súvisiacich s operačným systémom Windows.

Kritická zraniteľnosť CVE-2022-34691 umožňuje útočníkom eskaláciu oprávnení, pokiaľ na doméne beží služba Active Directory Certificate Services. Ostatné opravené kritické zraniteľnosti umožňujú vzdialené vykonávanie kódu. Zraniteľnosti CVE-2022-30133 a CVE-2022-35744 sa nachádzajú v protokole PPP (Point-to-Point) a útočník ich môže zneužiť odoslaním špeciálnej požiadavky RAS serveru. Zraniteľnosť CVE-2022-34696 sa nachádza vo virtualizačnej platforme Hyper-V. Zraniteľnosti CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767 a CVE-2022-35794 sa nachádzajú v protokole SSTP. Posledná kritická zraniteľnosť CVE-2022-35804 sa nachádza v protokole SMBv3 a útočník ju môže zneužiť pomocou špeciálnych požiadaviek tak na server ako aj na klientske zariadenie.

Zraniteľnosti vysokej závažnosti umožňujú vzdialené vykonávanie kódu, eskaláciu oprávnení a obídenie bezpečnostných prvkov. Zneužitie niektorých z nich môže viesť k úniku informácií a vyvolaniu nedostupnosti služby.

Zraniteľné systémy:

Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 21H1 for 32-bit Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 21H2 for 32-bit Systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 Version 21H2 for x64-based Systems
Windows 11 for ARM64-based Systems
Windows 11 for x64-based Systems
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
Windows RT 8.1

Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows Server 2019
Windows Server 2019 (Server Core installation)
Windows Server 2022
Windows Server 2022 (Server Core installation)
Windows Server, version 20H2 (Server Core Installation)

Odporúčania:

Odporúčame aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania.

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34691
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30133
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34696
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34702
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34714
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35744
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35745
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35752
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35753
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35766
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35767
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35794
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35804

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci august 4 závažné zraniteľnosti. Zraniteľnosť CVE-2022-33631 v produkte Microsoft Excel umožňuje útočníkovi obchádzať bezpečnostné prvky. Zraniteľnosti CVE-2022-33648 a CVE-2022-34717 v balíku Microsoft Office umožňujú vzdialene vykonávať kód. Zneužitie zraniteľnosť CVE-2022-35742 môže spôsobiť nedostupnosť služby.

Zraniteľné systémy:

Microsoft 365 Apps for Enterprise for 32-bit Systems

Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office Online Server
Microsoft Outlook 2013 RT Service Pack 1
Microsoft Outlook 2013 Service Pack 1 (32-bit editions)
Microsoft Outlook 2013 Service Pack 1 (64-bit editions)
Microsoft Outlook 2016 (32-bit edition)
Microsoft Outlook 2016 (64-bit edition)

Odporúčania:
Odporúčame aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft ukončila podporu prehliadača Internet Explorer 15.6.2022 pre hlavnú líniu operačných systémov Windows 10. Pre zvyšné operačné systémy, kde je prehliadač ešte podporovaný, nevydala v mesiaci august žiadne opravy kritických a závažných zraniteľností.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac v prehliadači Edge jednu závažnú zraniteľnosť. Zraniteľnosti CVE-2022-33649 umožňuje útočníkom obchádzať bezpečnostné prvky aplikácie, konkrétne môže viesť k úniku zo sandboxu prehliadača. Pre jej zneužitie musí útočník presvedčiť obeť, aby navštívila škodlivú webstránku alebo otvorila škodlivú prílohu.

Zraniteľné systémy:

Microsoft Edge (Chromium-based)

Odporúčania:

Odporúčame aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania.

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-33649

Mozilla Firefox

V mesiaci august boli v prehliadači Firefox a Firefox ESR opravené 4 závažné zraniteľnosti.

Závažná zraniteľnosť CVE-2022-38472 umožňuje útočníkovi podvrhnúť škodlivý obsah ako obsah adresného riadka zneužitím spôsobu narábania s chybami XSLT.

Zraniteľnosť CVE-2022-38473 spôsobuje, že XSLT dokumentu z cudzieho zdroja sú pridelené oprávnenia rodičovskej domény. Môže sa jednať napríklad o prístup k mikrofónu a kamere.

Zraniteľnosti CVE-2022-38477 a CVE-2022-38478 sú sady zraniteľností ovplyvňujúcich bezpečnosť pamäte, ktoré môžu viesť ku poškodeniu pamäte alebo možnosti vykonávať kód.

Zraniteľné systémy:

Mozilla Firefox verzie staršej ako 104
Mozilla Firefox ESR verzie staršej ako 102.2

Odporúčania:

Odporúčame aktualizáciu Firefox na verziu 104 a Firefox ESR na verziu 102.2

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-33/

Google Chrome

V mesiaci august bola vydaná oprava 2 kritických a 23 závažných zraniteľností. Kritické zraniteľnosti CVE-2022-2852 v komponente FedCM a CVE-2022-3038 v komponente Network Service umožňujú použitie dealokovaného miesta v pamäti.

Závažné zraniteľnosti umožňujú použiť dealokované miesto v pamäti, zapisovať do pamäte mimo povolené hodnoty, vedú ku pretečeniu medzipamäte haldy, či súvisia s nedostatočným overovaním nedôveryhodných vstupov.

Zraniteľné systémy:
Google Chrome pre Windows, Mac a Linux verzie staršej ako 105.0.5195.52.

Odporúčania:
Odporúčame aktualizáciu prehliadača Chrome pre Windows, Mac a Linux aspoň na verziu 105.0.5195.52.

Zdroje:
https://chromereleases.googleblog.com/2022
https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html
https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html
https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html

4. Adobe Acrobat a Reader

V produkte Adobe Acrobat a Reader neboli v mesiaci august opravené žiadne kritické ani závažné zraniteľnosti.

Zdroje:
https://helpx.adobe.com/security.html

5. Frameworky

Microsoft .NET Framework

V mesiaci august spoločnosť Microsoft neopravila žiadnu kritickú ani závažnú zraniteľnosť vo frameworku .NET.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance

Oracle Java

Veľká sada opráv je plánovaná na 18. október 2022.

Zdroje:
https://www.oracle.com/technetwork/topics/security/alerts-086861.html

6. Iné závažné zraniteľnosti

Kritické zraniteľnosti routerov Cisco Small Business

Spoločnosť CISCO opravila 2 kritické a jednu závažnú zraniteľnosť malých podnikových bezpečnostných smerovačov (routerov série RV), ktoré umožňujú vzdialené pripájanie k podnikovej infraštruktúre službou VPN. Potenciálny útočník by mohol po úspešnom zneužití zraniteľnosti vykonávať ľubovoľný kód, či príkazy, a tak vytvoriť podmienky aj pre nedostupnosť služby. VJ CSIRT odporúča čo najskôr aktualizovať firmvér zraniteľných sieťových prvkov. Viac informácií na stránke.

Zimbra – aktívne zneužívané závažné zraniteľnosti

Podľa spoločnosti Volexity útočníci aktívne zneužívajú zraniteľné servery Zimbra. Útočníci zreťazujú závažné zraniteľnosti, ktoré im umožňujú neoprávnene pristúpiť na server a vzdialene vykonávať škodlivý kód – nasadiť na server web shell. Podľa spoločnosti Volexity je aktuálne z verejného internetu dostupných viac ako 1 000 kompromitovaných Zimbra serverov. VJ CSIRT odporúča skontrolovať servery Zimbra na prítomnosť kompromitácie a nasadiť bezpečnostné záplaty na zraniteľné inštancie. Viac informácií na stránke.

Závažné zraniteľnosti bezpečnostných produktov Cisco

Spoločnosť Cisco vydala aktualizácie opravujúce závažné zraniteľnosti produktov Cisco ASA, Firepower či manažmentového softvéru Cisco ASDM. Úspešné zneužitie zraniteľností by mohlo umožniť útočníkovi odcudziť citlivé dáta zariadení, narušiť bezpečnosť šifrovanej komunikácie alebo kompromitovať klientske zariadenie správcu. Viac informácií na stránke.

Možnosti vzdialeného prístupu – alebo ako (ne)otvoriť dvere útočníkovi do podnikovej siete

Spravodajská spoločnosť Cyble venujúca sa dark webu varuje, že zaznamenala nárast kybernetických útokov zameraných na virtuálne vzdialené pripojenie VNC. Služba VNC a jej protokol RFB (Remote Frame Buffer) poskytuje vzdialený prístup na virtuálny počítač, čo je funkcionalita, ktorá je aj v čase pandémie aktívne využívaná na vzdialené pripájanie k podnikovým sieťam/virtuálnemu pracovnému prostrediu. VJ CSIRT varuje pred nedostatočným zabezpečením možností vzdialeného pripájania k podnikovým sieťam či službám. Protokoly a služby ako VNC, RDP, FTP, SMB a pod. by nemali byť priamo dostupné z verejného internetu. Viac informácií na stránke.