MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

AUGUST 2024

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci august 6 kritických a 60 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritická zraniteľnosť v komponente Windows TCP/IP spočíva v podtečení celočíselnej premennej. CVE-2024-38063 by vzdialený neautentifikovaný útočník prostredníctvom zaslania špeciálne vytvorených IPv6 paketov mohol zneužiť na vzdialené vykonanie škodlivého kódu. Zraniteľnosť je možné zneužiť len na systémoch s aktivovaným IPv6 a možno ju mitigovať vypnutím podpory IPv6.

Komponent RMCAST (Windows Reliable Multicast Transport Driver) obsahuje zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu. Zraniteľnosť CVE-2024-38140 je možné zneužiť len v prípade, že je na zraniteľných systémoch aktivovaná funkcia PGM (Pragmatic General Multicast) a ľubovoľná aplikácia počúva na PGM porte. Nakoľko PGM vo všeobecnosti neautentifikuje prichádzajúce požiadavky, Microsoft odporúča limitovať prístup k PGM portu prostredníctvom sieťových bezpečnostných prvkov a neponechávať ho verejne dostupný.

Kritické zraniteľnosti s označením CVE-2024-38159 a CVE-2024-38160 nachádzajúce sa v komponente Windows Network Virtualization spočívajú v použití odalokovaného miesta v pamäti a pretečení medzipamäte haldy. Vzdialený autentifikovaný útočník by ich mohol prostredníctvom úpravy obsahu MDL (Memory Descriptor List) zneužiť na vzdialené vykonanie škodlivého kódu. Zneužitie zraniteľnosti vyžaduje vysoké privilégiá umožňujúce manipuláciu bežiacich procesov.

Spoločnosť Microsoft opravila aj zraniteľnosti linuxových nástrojov grub2 (CVE-2022-3775) a shim (CVE-2023-40547), ktoré umožňovali obídenie bezpečnostných mechanizmov Secure Boot a následné vykonanie škodlivého kódu.

Ostatné zraniteľnosti vysokej závažnosti umožňujú vzdialené vykonanie škodlivého kódu, eskaláciu privilégií, zneprístupnenie služby, obídenie bezpečnostného prvku, získanie neoprávneného prístupu k citlivým údajom alebo vykonanie neoprávnených zmien v systéme.

ZRANITEĽNÉ SYSTÉMY:

- Remote Desktop client for Windows Desktop
- 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 21H2 for 32-bit Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 10 for 32-bit Systems
- Windows 10 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems
- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 23H2 for ARM64-based Systems
- Windows 11 Version 23H2 for x64-based Systems
- Windows 11 Version 24H2 for ARM64-based Systems
- Windows 11 Version 24H2 for x64-based Systems
- Windows 11 version 21H2 for ARM64-based Systems
- Windows 11 version 21H2 for x64-based Systems
- 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 2022, 23H2 Edition (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://msrc.microsoft.com/update-guide/en-us
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3775
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-40547
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38140
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38159
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38160

Koniec podpory pre Windows Server 2012 a Windows Server 2012 R2

Spoločnosť Microsoft plánovane zrušila podporu pre Windows Server 2012 a Windows Server 2012 R2. Po dátume 10. októbra 2023 už tieto produkty nebudú dostávať aktualizácie zabezpečenia, aktualizácie nesúvisiace so zabezpečením, opravy chýb, technickú podporu a ani aktualizácie technického obsahu online.

ODPORÚČANIA:

Administrátorom a používateľom systémov Windows Server 2012 a Windows Server 2012 R2 odporúčame prejsť na novšiu verziu operačného systému alebo používať rozšírenie ESU na dobu určitú. Viac informácií na stránke.

2. KANCELÁRSKE BALÍKY MICROSOFT OFFICE A OFFICE WEB APPS

Spoločnosť Microsoft vydala v mesiaci august bezpečnostné aktualizácie, ktoré opravujú 1 kritickú a 10 vysoko závažných zraniteľnosti v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Zraniteľnosť CVE-2024-38206 v produkte Microsoft Copilot Studio by vzdialený autentifikovaný útočník mohol zneužiť obídenie bezpečnostných mechanizmov ochrany pred SSRF (Server Side Request Forgery) a získanie neoprávneného prístupu k citlivým údajom. Zraniteľnosť bola odstránená spoločnosťou Microsoft a nie je potrebná dodatočná aktivita zo strany používateľov.

Zraniteľnosť v produkte Microsoft OfficePlus (CVE-2024-38084) spočíva v nesprávnom overovaní odkazov pred prístupom k súborom a lokálny autentifikovaný používateľ by ju mohol zneužiť na eskaláciu privilégií na úroveň používateľa SYSTEM.

Zraniteľnosti v produktoch Microsoft Office Visio (CVE-2024-38169), Microsoft Excel (CVE-2024-38170, CVE-2024-38172), Microsoft Project (CVE-2024-38189) a Microsoft PowerPoint (CVE-2024-38171) spočívajú v pretečení medzipamäte haldy, použití odalokovaného miesta v pamäti a nesprávnom overovaní vstupov a vzdialený útočník by ich mohol zneužiť na vzdialené vykonanie kódu. Zneužitie zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí stiahnuť a otvoriť špeciálne vytvorený súbor.

Microsoft Outlook obsahuje tzv. Form Injection zraniteľnosť, ktorú by vzdialený autentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu. Na zneužitie CVE-2024-38173 útočník musí získať prístup k Outlook účtu obete a následne nainštalovať škodlivý formulár. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť škodlivý e-mail v zraniteľnej verzii Outlook. Na systémoch s aktivovanou funkciou automatického otvárania e-mailov sa jedná o tzv. zero-click zraniteľnosť, ktorá nevyžaduje interakciu používateľa.

Zraniteľnosť s označením CVE-2024-38177 v komponente Windows App Installer by vzdialený útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na úplné narušenie dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa, ktorý musí prostredníctvom škodlivého winget súboru spustiť Windows App Installer.

CVE-2024-38197 v produkte Microsoft Teams for iOS by vzdialený neautentifikovaný útočník mohol zneužiť na modifikáciu mena odosielateľa správ aplikácie Teams a využitím princípov sociálneho inžinierstva v rámci komunikácie získať neoprávnený prístup k citlivým údajom.

CVE-2024-38200 v produktoch Microsoft Office a Microsoft 365 by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu alebo súboru

mohol zneužiť na získanie autentifikačných NTLM hashov. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa, ktorý musí kliknúť na URL odkaz alebo otvoriť špeciálne vytvorený súbor. Zneužitie zraniteľnosti je možné mitigovať aj aktiváciou bezpečnostnej politiky pre blokovanie odchádzajúcej NTLM komunikácie na vzdialené servery, pridaním používateľov do skupiny Protected Users Security Group alebo blokovaním odchádzajúcej komunikácie TCP 445/SMB prostredníctvom sieťových alebo bezpečnostných prvkov.

ZRANITEĽNÉ SYSTÉMY:

- App Installer
- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft Copilot Studio
- 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 LTSC for Mac 2021
- Microsoft OfficePLUS
- Microsoft Outlook 2016 (32-bit edition)
- Microsoft Outlook 2016 (64-bit edition)
- Microsoft PowerPoint 2016 (32-bit edition)
- Microsoft PowerPoint 2016 (64-bit edition)
- Microsoft Project 2016 (32-bit edition)
- Microsoft Project 2016 (64-bit edition)
- Microsoft Teams for iOS

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-2024-38206
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38084
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38169
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38170
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38171
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38172
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38173
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38177
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38189
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38197
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38200

3. INTERNETOVÉ PREHLIADAČE

MICROSOFT INTERNET EXPLORER

Spoločnosť Microsoft ukončila podporu prehliadača Internet Explorer 15.6.2022 pre hlavnú líniu operačných systémov Windows 10 a 11. Spoločnosť Microsoft za mesiac máj neopravila žiadne kritické ani vysoko závažné zraniteľnosti pre zvyšné operačné systémy podporujúce Internet Explorer.

ODPORÚČANIA:

Odporúčame prestať používať a odinštalovať Internet Explorer a nahradiť ho podporovaným prehliadačom Microsoft Edge.

ZDROJE:

- https://msrc.microsoft.com/update-guide/en-us

MICROSOFT EDGE

Text Spoločnosť Microsoft v mesiaci august opravila 3 vysoko závažné zraniteľnosti vo webovom prehliadači Microsoft Edge.

Zraniteľnosti s označením CVE-2024-38209, CVE-2024-38210 a CVE-2024-38218 by vzdialený útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vykonanie škodlivého kódu. Zneužitie zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí škodlivý súbor otvoriť na zraniteľnom zariadení.

ZDROJE:

- https://msrc.microsoft.com/update-guide/en-us
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38209
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38210
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38218

MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci august opravila 11 vysoko závažných zraniteľností v línii internetových prehliadačov Firefox a Firefox ESR.

Zraniteľnosti s označením CVE-2024-7519, CVE-2024-7520, CVE-2024-7527, CVE-2024-7528, CVE-2024-7521, CVE-2024-7522 v líniách Firefox a Firefox ESR spočívajú v nesprávnej kontrole pri spracovaní zdieľanej grafickej pamäti, nesprávnom vyhodnocovaní dátových typov, použití odalokovaného miesta v pamäti a čítaní mimo povolených hodnôt a vzdialený neautentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu zneužiť na vykonanie škodlivého kódu.

Zraniteľnosti CVE-2024-7523 (línia Firefox), CVE-2024-7524 a CVE-2024-7525 (Firefox, Firefox ESR) možno zneužiť na obídenie bezpečnostných mechanizmov webového prehliadača, injekciu HTML elementov a realizáciu XSS (Cross Site Scripting) útokov.

Komponent ANGLE (CVE-2024-7526) obsahuje zraniteľnosti spočívajúce v čítaní neinicializovaného obsahu pamäti a možno ich zneužiť na získanie neoprávneného prístupu k citlivým údajom.

Zraniteľnosť CVE-2024-7518 by útočník mohol zneužiť na obídenie výzvy na zobrazenie obsahu na celú obrazovku, narušenie integrity zobrazovaného obsahu a realizáciu spoofing útokov.

Zneužitie všetkých zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť špeciálne vytvorený webový obsah.

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox verzie staršie ako 129
- Mozilla Firefox ESR verzie staršej ako 128.1

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 129 a Firefox ESR na verziu 128.1.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-33/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-34/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-35/
- https://exchange.xforce.ibmcloud.com/vulnerabilities/350605
- https://exchange.xforce.ibmcloud.com/vulnerabilities/350604
- https://exchange.xforce.ibmcloud.com/vulnerabilities/350612
- https://exchange.xforce.ibmcloud.com/vulnerabilities/350613
- https://exchange.xforce.ibmcloud.com/vulnerabilities/350606
- https://exchange.xforce.ibmcloud.com/vulnerabilities/350607
- https://exchange.xforce.ibmcloud.com/vulnerabilities/350610
- https://exchange.xforce.ibmcloud.com/vulnerabilities/350608
- https://exchange.xforce.ibmcloud.com/vulnerabilities/350609
- https://exchange.xforce.ibmcloud.com/vulnerabilities/350611
- https://exchange.xforce.ibmcloud.com/vulnerabilities/350603

GOOGLE CHROME

V mesiaci august spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili celkom 1 kritickú a 15 vysoko závažných zraniteľností.

Nesprávnu implementáciu bezpečnostných mechanizmov (CVE-2024-7965, CVE-2024-7535) a nesprávne vyhodnocovanie typov (CVE-2024-7971, CVE-2024-7969, CVE-2024-8194, CVE-2024-7550) v komponente V8 by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu mohol zneužiť na obídenie bezpečnostných prvkov a vykonanie škodlivého kódu. Zraniteľnosti s označením CVE-2024-7965 a CVE-2024-7971 sú podľa spoločnosti Google v súčasnosti aktívne zneužívaná útočníkmi.

Zraniteľnosti v komponentoch Sharing (CVE-2024-7533), WebAudio (CVE-2024-7536), Passwords (CVE-2024-7964) a Autofill (CVE-2024-7968) spočívajú v použití odalokovaného miesta v pamäti a možno ich zneužiť vzdialené vykonanie škodlivého kódu.

Pretečením zásobníka haldy v komponentoch Fonts (CVE-2024-7967), Layouts (CVE-2024-7534) a Skia (CVE-2024-8193, CVE-2024-8198) možno spôsobiť pád prehliadača alebo vykonať škodlivý kód.

Zraniteľnosti s označením CVE-2024-7532 a CVE-2024-7966 spočívajú v čítaní obsahu pamäte mimo povolených hodnôt a umožňujú vzdialené vykonanie škodlivého kódu.

Zneužitie všetkých vyššie uvedených zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť špeciálne vytvorený webový obsah.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows a Mac verzie staršej ako 128.0.6613.113/.114
- Google Chrome pre Linux verzie staršej ako 128.0.6613.113

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 128.0.6613.113/.114 a Linux verzie aspoň na verziu 128.0.6613.113.

ZDROJE:

- https://chromereleases.googleblog.com/2024
- https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_28.html
- https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
- https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_13.html
- https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop.html
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351762
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351752

- https://exchange.xforce.ibmcloud.com/vulnerabilities/351754
- https://exchange.xforce.ibmcloud.com/vulnerabilities/352211
- https://exchange.xforce.ibmcloud.com/vulnerabilities/350527
- https://exchange.xforce.ibmcloud.com/vulnerabilities/350523
- https://exchange.xforce.ibmcloud.com/vulnerabilities/350526
- https://exchange.xforce.ibmcloud.com/vulnerabilities/350525
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351758
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351756
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351764
- https://exchange.xforce.ibmcloud.com/vulnerabilities/350524
- https://exchange.xforce.ibmcloud.com/vulnerabilities/352210
- https://exchange.xforce.ibmcloud.com/vulnerabilities/352209
- https://exchange.xforce.ibmcloud.com/vulnerabilities/350528
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351759

4. ADOBE ACROBAT A READER

V mesiaci august spoločnosť Adobe vydala bezpečnostné aktualizácie, ktoré opravili celkom 12 zraniteľností v produktoch Adobe Acrobat a Reader, z toho 8 kritických a 4 boli označené ako vysoko závažné.

Kritické zraniteľnosti s označením CVE-2024-39383, CVE-2024-39422, CVE-2024-39423, CVE-2024-39424, CVE-2024-39425, CVE-2024-39426, CVE-2024-41830 a CVE-2024-41831 spočívajú v použití odalokovaného miesta v pamäti, zápise mimo povolených hodnôt a nedostatočnom overovaní kryptografických podpisov. Vzdialený neautentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vzdialené vykonanie škodlivého kódu alebo zneprístupnenie služby.

Vysoko závažné zraniteľnosti s označením CVE-2024-41832, CVE-2024-41833, CVE-2024-41834 a CVE-2024-41835 spočívajú v čítaní mimo povolených hodnôt a vzdialený útočník by ich prostredníctvom podvrhnutia špeciálne vytvorených dokumentov mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom.

Zneužitie všetkých zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť škodlivý súbor.

ZDROJE:

- https://helpx.adobe.com/security/security-bulletin.html#acrobat
- https://helpx.adobe.com/security/products/acrobat/apsb24-57.html
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351346
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351347
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351348
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351349
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351351
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351352
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351353
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351350
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351354
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351355
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351356
- https://exchange.xforce.ibmcloud.com/vulnerabilities/351357

5. FRAMEWORKY

MICROSOFT .NET FRAMEWORK

V mesiaci august spoločnosť Microsoft neopravila žiadne kritické ani vysoko závažné zraniteľnosti vo frameworku .NET.

ZDROJE:

- https://msrc.microsoft.com/update-guide/en-us

ORACLE JAVA

Veľká sada opráv je plánovaná na 15. októbra 2024.

6. INÉ ZÁVAŽNÉ ZRANITĽNOSTI

KRITICKÁ ZRANITEĽNOSŤ FORTRA FILECATALYST WORKFLOW

Fortra FileCatalyst Workflow obsahuje kritickú zraniteľnosť, ktorá umožňuje vzdialeným útočníkom administrátorský prístup ku prednastavenej databáze softvéru, čím môžu získať úplnú kontrolu nad zraniteľnou webovou aplikáciou. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V DOPLNKU WORDPRESS WPML

Vývojári populárneho doplnku WordPress WPML slúžiaceho na vytváranie viacjazyčných stránok vydali bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť. Zraniteľnosť s označením CVE-2024-6386 umožňuje vykonanie škodlivého kódu a získanie úplnej kontroly nad inštanciou redakčného systému WordPress. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ ZRANITEĽNOSŤ V GOOGLE CHROME

Spoločnosť Google vydala bezpečnostné aktualizácie na svoj webový prehliadač Chrome, ktoré opravujú 19 zraniteľností. Najzávažnejšie zraniteľnosti v komponentoch V8, Passwords, Skia, Fonts a Autofill možno zneužiť umožňujú vzdialené vykonanie kódu a zneprístupnenie služby. Zraniteľnosť s označením CVE-2024-7965 je aktívne zneužívaná útočníkmi. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V PRODUKTE SOLARWINDS

Spoločnosť SolarWinds vydala bezpečnostné aktualizácie pre službu Web Help Desk (WHD), ktoré opravujú kritické zraniteľnosti s označením CVE-2024-28986 a CVE-2024-228987. Vzdialený útočník ich môže zneužiť na vzdialené vykonávanie kódu a neoprávnený prístup do systému. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V MODULE WORDPRESS GIVEWP

Modul WordPress GiveWP, ktorý poskytuje možnosť vytvorenia darcovského rozhrania na webstránkach, obsahuje kritickú zraniteľnosť súvisiacu s nedostatočným overovaním používateľských vstupov. Jej zneužitím dokáže útočník vzdialene vykonávať kód a mazať súbory. Môže získať úplnú kontrolu nad zraniteľnou inštanciou WordPress. Viac informácií na stránke.

MICROSOFT ODHALIL BEZPEČNOSTNÉ ZRANITEĽNOSTI V OPENVPN

Bezpečnostní výskumníci zo spoločnosti Microsoft na hackerskej konferencii Black Hat USA 2024 zverejnili informácie o 4 zraniteľnostiach OpenVPN, ktorých zreťazením by vzdialený útočník mohol získať úplnú kontrolu nad systémom. Vývojári OpenVPN zraniteľnosti opravili ešte v marci 2024 vydaním verzie 2.6.10. Viac informácií na stránke.

MICROSOFT V RÁMCI AUGUSTOVÉHO PATCH TUESDAY OPRAVIL 9 KRITICKÝCH ZRANITEĽNOSTÍ

Spoločnosť Microsoft vydala v auguste 2024 balík opráv pre portfólio svojich produktov opravujúci 90 zraniteľností, z ktorých 24 umožňuje vzdialené vykonávanie kódu. Kritické zraniteľnosti sa nachádzajú v produktoch Microsoft Dynamics 365, Microsoft Copilot Studio a Azure Health Bot a v komponentoch grub2, shim, Windows TCP/IP, Windows Reliable Multicast Transport Driver a Windows Network Virtualization. Zraniteľnosti s označením CVE-2024-38189, CVE-2024-38178, CVE-2024-38193, CVE-2024-38106, CVE-2024-38107 a CVE-2024-38213 sú aktívne zneužívané útočníkmi. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V PRODUKTOCH SAP

Spoločnosť SAP vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú 17 zraniteľností, z toho 2 sú označené ako kritické. Kritické zraniteľnosti sa nachádzajú v produktoch SAP BusinessObjects Business Intelligence Platform a SAP Build Apps a možno ich zneužiť na realizáciu SSRF útokov a získanie neoprávneného prístupu do systému.. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V IVANTI VIRTUAL TRAFFIC MANAGER A IVANTI NEURONS FOR ITSM

Spoločnosť Ivanti vydala bezpečnostné aktualizácie pre svoje produkty Virtual Traffic Manager a Neurons for ITSM, ktoré opravujú 3 bezpečnostné zraniteľnosti, z toho 2 sú označené ako kritické. Zneužitím zraniteľností je možné získať neoprávnený prístup do systému a k citlivým údajom. Viac informácií na stránke.

ZRANITEĽNOSTI NÁSTROJA PRE SPRÁVU HESIEL 1PASSWORD PRE MACOS

Vývojári nástroja pre správu hesiel 1Password for Mac vydali bezpečnostné aktualizácie, ktoré opravujú dve bezpečnostné zraniteľnosti umožňujúce získanie neoprávneného prístupu k uloženým heslám. CVE-2024-42218 a CVE-2024-42219 možno zneužiť na obídenie bezpečnostných mechanizmov operačného systému macOS a mechanizmov riadenia vzájomnej komunikácie medzi procesmi. Viac informácií na stránke.

18 ROKOV STARÁ ZRANITEĽNOSŤ „0.0.0.0“

Výskumný tím spoločnosti Oligo Security poukázal na zraniteľnosť s názvom “0.0.0.0 Day”, ktorá ovplyvňuje webové prehliadače Google Chrome, Mozilla Firefox, Apple Safari a prehliadače na báze Chromium. Zraniteľnosť umožňuje škodlivým webovým stránkam obchádzať zabezpečenie prehliadača a komunikovať so službami spustenými v lokálnej sieti. Útočníkovi umožňuje získanie neoprávneného prístupu k lokálnym službám a vzdialené vykonanie kódu. Zraniteľnosť je známa od roku 2006. Viac informácií na stránke.

ZRANITEĽNOSŤ MS OFFICE A 365 UMOŽŇUJÚCA ZÍSKANIE NTLM HASHOV

Spoločnosť Microsoft zverejnila informácie a odporúčania pre mitigáciu zraniteľnosti MS Office a MS 365 Apps, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na exfiltráciu NTLM hashov používaných v rámci autentifikácie. Viac informácií na stránke.

ZRANITEĽNOSŤ „SINKCLOSE“ V PROCESOROCH AMD

Spoločnosť AMD varuje pred vysoko závažnou zraniteľnosťou procesora, známou ako „SinkClose“. Táto chyba ovplyvňuje všetky procesory AMD vyrobené od roku 2006 a umožňuje útočníkom zvyšovanie privilégií a ľubovoľné vykonávanie kódu. Viac informácií na stránke.

KRITICKÁ BEZPEČNOSTNÁ ZRANITEĽNOSŤ V OPENSSH

Vývojári operačného systému FreeBSD vydali bezpečnostné aktualizácie, ktoré opravujú ďalší variant zraniteľnosti CVE-2024-6387 s označením CVE-2024-7589, ktorý možno taktiež zneužiť na vzdialené vykonanie škodlivého kódu. Viac informácií na stránke.

ZERO DAY ZRANITEĽNOSTI WINDOWS VEDÚ K DOWNGRADE SYSTÉMU

Bezpečnostný výskumník spoločnosti SafeBreach Alon Leviev na konferencii Black Hat 2024 odhalil dve zero-day zraniteľnosti. Vysoko závažné zraniteľnosti sa týkajú zvyšovania privilégií v systéme Windows Backup (VBS) vrátane podmnožiny Azure Virtual Machine SKUS. Viac informácií na stránke.

ZRANITEĽNOSTI V ROUNDCUBE UMOŽŇUJÚ EXFILTRÁCIU CITLIVÝCH ÚDAJOV A ROZPOSIELANIE E-MAILOV

Populárna webmailová platforma Roundcube obsahuje tri vysoko závažné zraniteľnosti, ktoré by vzdialený neautentifikovaný útočník zaslaním škodlivého e-mailu mohol zneužiť na realizáciu XSS útoku, získanie perzistencie v systéme obete, krádež citlivých údajov a rozposielanie e-mailových správ. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ ZRANITEĽNOSŤ V JADRE ANDROID

Spoločnosť Google vydala balík opráv pre OS Android, ktorý okrem iného rieši vysoko závažnú zero-day zraniteľnosť jadra, umožňujúcu vzdialené vykonávanie kódu. Zraniteľnosť je pravdepodobne zneužívaná pri cielených útokoch. Viac informácií na stránke.