Mesačný prehľad kritických zraniteľností
Máj 2024

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci máj 46 vysoko závažných zraniteľností v operačných systémov Windows.

Vysoko závažné zraniteľnosti s označením CVE-2024-29997, CVE-2024-29998, CVE-2024-29999, CVE-2024-30000, CVE-2024-30001, CVE-2024-30002, CVE-2024-30003, CVE-2024-30004, CVE-2024-30005, CVE-2024-30012 a CVE-2024-30021 nachádzajúce sa v komponente Mobile Broadband Driver umožňujú vykonanie škodlivého kódu. Zneužitie zraniteľností vyžaduje pripojenie škodlivého USB zariadenia do zraniteľného systému.

Komponenty WDAC OLE DB provider for SQL Server a Routing and Remote Access Service obsahujú zraniteľnosti CVE-2024-30006, CVE-2024-30009, CVE-2024-30014, CVE-2024-30015, CVE-2024-30022, CVE-2024-30023, CVE-2024-30024 a CVE-2024-30029, ktoré by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie kódu. Zneužitie zraniteľností vyžaduje interakciu zo strany používateľa, ktorý sa musí pripojiť na škodlivý server pod kontrolou útočníka.

Zraniteľnosti v hypervízore Hyper-V (CVE-2024-30010, CVE-2024-30017) a komponente Cryptographic Services (CVE-2024-30020) taktiež umožňujú vzdialené vykonanie kódu.

Ostatné zraniteľnosti vysokej závažnosti umožňujú eskaláciu privilégií, zneprístupnenie služby, obchádzanie bezpečnostných prvkov alebo získanie neoprávneného prístupu k citlivým údajom.

Zraniteľné systémy:

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 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

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 máj bezpečnostné aktualizácie, ktoré opravujú 1 kritickú a 4 vysoko závažné zraniteľnosti v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritická zraniteľnosť v produkte Microsoft SharePoint Server (CVE-2024-30044) umožňuje vzdialenému autentifikovanému útočníkovi s oprávneniami „Site Owner“ vykonať škodlivý kód v kontexte servera SharePoint. Zraniteľnosť je možné zneužiť uploadovaním špeciálne vytvoreného súboru a následným zaslaním špeciálne vytvorenej API požiadavky, ktorá vedie k deserializácii parametrov tohto súboru.

Microsoft SharePoint Server obsahuje aj vysoko závažnú zraniteľnosť CVE-2024-30043, ktorú možno zneužiť na získanie neoprávneného prístupu k citlivým údajom.

CVE-2024-30042 v produkte Microsoft Excel spočíva v deserializácii údajov a umožňuje vzdialené vykonanie kódu. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa, ktorý musí stiahnuť a otvoriť špeciálne vytvorený súbor.

Zraniteľnosť v produkte Microsoft Intune for Android Mobile s označením CVE-2024-30059 sa nachádza v komponente Mobile Application Management a možno ju zneužiť na obídenie bezpečnostných mechanizmov a získanie neoprávneného prístup k citlivým údajom. Na zneužitie zraniteľnosti by lokálny autentifikovaný útočník potreboval prístup k rootnutému zariadeniu, na ktorom by musel deaktivovať bližšie nešpecifikované časti zraniteľného komponentu.

Zneužitím zraniteľnosti CVE-2024-30041 v produkte Bing Search by útočník dokázal obeť presmerovať na webové stránky so škodlivým obsahom.

Zraniteľné systémy:

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Bing Search for iOS
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Intune Mobile Application Management for Android
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 SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Office Online Server

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-2024-30044
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30041
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30042
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30043
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30059
https://exchange.xforce.ibmcloud.com/vulnerabilities/290553

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

Spoločnosť Microsoft v mesiaci máj opravila 1 vysoko závažnú zraniteľnosť v prehliadači Microsoft Edge.

Zraniteľnosť s označením CVE-2024-30056 by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvoreného URL odkazu mohol zneužiť na získanie citlivých údajov z webového prehliadača obete. Zneužitie zraniteľnosti vyžaduje interakciu zo strany obete.

Zdroje:

https://msrc.microsoft.com/update-guide/en-us
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30056
https://exchange.xforce.ibmcloud.com/vulnerabilities/292628

Mozilla Firefox

Spoločnosť Mozilla v mesiaci apríl opravila 2 vysoko závažné zraniteľnosti v línii internetových prehliadačov Firefox a Firefox ESR.

Zraniteľnosť CVE-2024-4367 (línie Firefox a Firefox ESR) sa nachádza v komponente PDF.js a spočíva v chýbajúcej kontrole typov pri spracovaní fontov. Zneužitie zraniteľnosti umožňuje vykonanie ľubovoľného JavaScript kódu v kontexte PDF.js.

CVE-2024-4764 sa nachádza v línii Firefox a spočíva v použití odalokovaného miesta v pamäti pri pripojení nového audio vstupu, ku ktorému pristupuje viacero WebRTC vláken. Zraniteľnosť možno zneužiť na vykonanie kódu.

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

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 126
Mozilla Firefox ESR verzie staršej ako 115.11

Odporúčania:
Odporúčame aktualizovať Firefox na verziu 126 a Firefox ESR na verziu 115.11.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-21/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-22/
https://exchange.xforce.ibmcloud.com/vulnerabilities/290483
https://exchange.xforce.ibmcloud.com/vulnerabilities/290482

Google Chrome
V mesiaci máj spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili celkom 18 vysoko závažných zraniteľností.

Zraniteľnosti sa nachádzajú v komponentoch ANGLE, Dawn, Keyboard Inputs, Media Session, Presentation API, Scheduling, Streams Visuals, V8, WebAudio a WebRTC a spočívajú v zámene typov, použití odalokovaného miesta v pamäti, pretečení medzipamäte haldy a čítaní a zápise mimo povolených hodnôt. Vzdialený neautentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu mohol zneužiť na vykonanie škodlivého kódu.

Zraniteľnosti s označením CVE-2024-4671, CVE-2024-4761, CVE-2024-4947, CVE-2024-5274 sú aktívne zneužívané útočníkmi.

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 125.0.6422.141/.142
Google Chrome pre Linux verzie staršej ako 125.0.6422.141

Odporúčania:
Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 125.0.6422.141/.142 a Linux verzie aspoň na verziu 125.0.6422.141.

Zdroje:
https://chromereleases.googleblog.com/2024/05
https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_30.html
https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_23.html
https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_21.html
https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_15.html
https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_13.html
https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_9.html
https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_7.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/290016
https://exchange.xforce.ibmcloud.com/vulnerabilities/290017
https://exchange.xforce.ibmcloud.com/vulnerabilities/290176

https://exchange.xforce.ibmcloud.com/vulnerabilities/290389
https://exchange.xforce.ibmcloud.com/vulnerabilities/290698
https://exchange.xforce.ibmcloud.com/vulnerabilities/290700
https://exchange.xforce.ibmcloud.com/vulnerabilities/291031
https://exchange.xforce.ibmcloud.com/vulnerabilities/291032
https://exchange.xforce.ibmcloud.com/vulnerabilities/291033
https://exchange.xforce.ibmcloud.com/vulnerabilities/291034
https://exchange.xforce.ibmcloud.com/vulnerabilities/292341
https://exchange.xforce.ibmcloud.com/vulnerabilities/292644
https://exchange.xforce.ibmcloud.com/vulnerabilities/292643
https://exchange.xforce.ibmcloud.com/vulnerabilities/292645
https://exchange.xforce.ibmcloud.com/vulnerabilities/292646
https://exchange.xforce.ibmcloud.com/vulnerabilities/292647
https://exchange.xforce.ibmcloud.com/vulnerabilities/292648
https://exchange.xforce.ibmcloud.com/vulnerabilities/292649

4. Adobe Acrobat a Reader

V produkte Adobe Acrobat a Reader bolo v mesiaci máj opravených 11 kritických a 2 vysoko závažné zraniteľnosti.

Kritické bezpečnostné zraniteľnosti s označením CVE-2024-30279, CVE-2024-30280, CVE-2024-30284, CVE-2024-30310, CVE-2024-34094, CVE-2024-34095, CVE-2024-34096, CVE-2024-34097, CVE-2024-34098, CVE-2024-34099 a CVE-2024-34100 spočívajú v možnosti zapisovania a čítania mimo povolených hodnôt, použití odalokovaného miesta v pamäti a nesprávnej implementácii mechanizmov riadenia prístupu. Ich zneužitím možno vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

CVE-2024-30311 a CVE-2024-30312 možno zneužiť na získanie neopraveného prístupu k citlivým údajom.

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

Zraniteľné systémy:

Acrobat DC a Acrobat Reader DC pre Windows a Mac verzie 24.002.20736 a staršie,
Acrobat 2020 a Acrobat Reader 2020 pre Windows a Mac verzie 20.005.30574 a staršie.

Odporúčania:

Odporúčame aktualizáciu aspoň na verziu:
Acrobat DC a Acrobat Reader DC pre Windows a Mac 24.002.20759,
Acrobat 2020 a Acrobat Reader 2020 pre Windows 20.005.30636 a Mac 20.005.30635.

Zdroje:

https://helpx.adobe.com/security/security-bulletin.html#acrobat
https://helpx.adobe.com/security/products/acrobat/apsb24-29.html
https://nvd.nist.gov/vuln/search

5. Frameworky

Microsoft .NET Framework

V mesiaci máj spoločnosť Microsoft opravila 2 vysoko závažné zraniteľnosti vo frameworku .NET.

Zraniteľnosť s označením CVE-2024-30045 spočíva v pretečení medzipamäte haldy a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvoreného obsahu mohol zneužiť na vykonanie kódu. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa.

CVE-2024-30046 spočíva v súbežnom využívaní zdieľaných zdrojov a možno ju zneužiť na zneprístupnenie služby.

Zraniteľné systémy:

.NET 7.0
.NET 8.0

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-2024-30045
https://exchange.xforce.ibmcloud.com/vulnerabilities/290582
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30046

Oracle Java

Veľká sada opráv je plánovaná na 16. júla 2024.

6. Iné závažné zraniteľnosti

Aktívne zneužívaná zraniteľnosť bezpečnostných brán Check Point

Spoločnosť Check Point vydala bezpečnostné aktualizácie pre aktívne zneužívanú zraniteľnosť vedúcu k úniku citlivých informácií, zneužiteľných na prienik do siete a laterálny pohyb v nej. Zraniteľnosť zasahuje bezpečnostné brány Network Security Gateway s povolenými službami Remote Access VPN a lebo Mobile Access. Útočníci môžu získať hashe hesiel používateľských účtov a prístup k Active Directory. Zneužitím exfiltrovaných údajov je možné dosiahnuť aj vzdialené vykonanie kódu. **Viac informácií na stránke**.

Zraniteľnosti v produktoch Veeam

Spoločnosť Veeam vydala bezpečnostné aktualizácie na svoje produkty Backup & Replication, Agent for Windows a Service Provider Console, ktoré opravujú viacero zraniteľností

umožňujúcich obchádzanie bezpečnostných prvkov, eskaláciu privilégií alebo vzdialené vykonanie kódu. **Viac informácií na stránke.**

Bezpečnostné zraniteľnosti v produktoch Ivanti

Spoločnosť Ivanti vydala bezpečnostné aktualizácie, ktoré opravujú 16 bezpečnostných zraniteľností v produktoch Avalanche, Neurons for ITSM, Neurons for ITAM, Connect Secure, Policy Secure, Secure Access a Endpoint Manager. Najzávažnejšie sú kritické zraniteľnosti v produkte Endpoint Manager, ktoré možno zneužiť na vykonanie škodlivého kódu. **Viac informácií na stránke.**

Aktívne zneužívané zero-day zraniteľnosti Google Chrome

Spoločnosť Google vydala bezpečnostné aktualizácie na opravu troch zero-day zraniteľností vo webovom prehliadači Chrome, ktoré možno zneužiť na vykonanie škodlivého kódu, zneprístupnenie služby alebo získanie neoprávneného prístupu k citlivým údajom. Zraniteľnosti sú aktívne zneužívané útočníkmi, odporúčame bezodkladnú aktualizáciu. **Viac informácií na stránke.**

Bezpečnostné zraniteľnosti v produktoch VMware Workstation a Fusion

Spoločnosť BROADCOM vydala bezpečnostné aktualizácie, ktoré opravujú 4 bezpečnostné zraniteľnosti v produktoch VMware Workstation a Fusion, z toho je 1 označená ako kritická. Zraniteľnosti možno zneužiť na vzdialené vykonanie škodlivého kódu, zneprístupnenie služby a neoprávnený prístup k citlivým údajom. **Viac informácií na stránke.**

Bezpečnostné zraniteľnosti v BIG-IP Next Central Manager

Spoločnosť F5 vydala bezpečnostné aktualizácie na svoj produkt BIG-IP Next Central Manager, ktoré možno zneužiť na vykonanie SQL a OData injekcie a následné získanie úplnej kontroly nad zraniteľnými systémami. **Viac informácií na stránke.**

Kritická zraniteľnosť manažmentového nástroja Veeam Service Provider Console

Spoločnosť Veeam vydala bezpečnostné aktualizácie, ktoré opravujú kritickú bezpečnostnú zraniteľnosť nástroja Veeam Service Provider Console, slúžiaceho na centralizovaný manažment prostredí využívajúcich technologické riešenia od Veeam. Zraniteľnosť možno zneužiť na vzdialené vykonanie kódu. **Viac informácií na stránke.**

Microsoft v rámci Patch Tuesday opravil aktívne zneužívané zero-day zraniteľnosti

Spoločnosť Microsoft vydala v máji 2024 balík opráv pre portfólio svojich produktov opravujúci 61 zraniteľností, z ktorých 28 umožňuje vzdialené vykonávanie kódu. Tri zraniteľnosti sú typu zero-day a dve z nich sú aktívne zneužívané. **Viac informácií na stránke.**

Kampaň botnetu „Goldoon“ zneužíva starú kritickú zraniteľnosť smerovačov D-Link

Bezpečnostní výskumníci z FortiGuard poukázali na novú útočnú kampaň šíriacu malvér/botnet Goldoon, ktorá sa zameriava na routery D-Link. Počas apríla sa dvojnásobne zvýšil nárast útokov na bezpečnostnú chybu s označením CVE-2015-2051. Zaujímavosťou je, že táto zraniteľnosť je už takmer desať rokov stará. **Viac informácií na stránke.**