Mesačný prehľad kritických zraniteľností november 2023

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci november 2 kritické a 30 vysoko závažných zraniteľností.

Kritická zraniteľnosť CVE-2023-36397 sa nachádza v službe Windows Message Queuing (MSMQ). Služba MSMQ systému Windows musí byť povolená, aby mohlo dôjsť k zneužitiu tejto zraniteľnosti. Útočník môže vzdialene vykonávať kód na strane servera odoslaním špeciálne upraveného súboru. Microsoft na zmiernenie zraniteľnosti odporúča službu MSMQ vypnúť. Či je služba aktívna môžete skontrolovať v aktívnych procesoch a či zariadenie počúva na porte TCP 1801.

Zraniteľnosť CVE-2023-36400 sa nachádza vo virtualizačnej platforme Hyper-V a umožňuje eskaláciu privilégií až na úroveň SYSTEM. Úspešné zneužitie umožňuje útočníkovi vykonať škodlivý kód na hostiteľskom serveri z hosťovského virtuálneho zariadenia s nízkymi oprávneniami.

Vysoko závažné zraniteľnosti umožňujú obchádzanie bezpečnostných prvkov, eskaláciu oprávnení a narušenie dostupnosti služby. Zneužitie niektorých z nich môže viesť k úniku informácií, vzdialenému vykonávaniu kódu alebo predstieraniu/falšovaniu identity.

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 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 11 version 21H2 for ARM64-based Systems
Windows 11 version 21H2 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 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-2023-36397
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36400

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci november 5 vysoko závažných zraniteľností.

Vysoko závažné zraniteľnosti CVE-2023-36037 a CVE-2023-36413 sa týkajú obídenia bezpečnostných prvkov v balíku Microsoft Office. Závažné zraniteľnosti CVE-2023-36041 (Excel), CVE-2023-36045 (Office Graphics) a CVE-2023-38177 (SharePoint Server) umožňujú vzdialené vykonávanie kódu.

Zraniteľné systémy:

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
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 SharePoint Enterprise Server 2016

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-2023-36037
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36041
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36045
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36413
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38177

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. Pre zvyšné operačné systémy, kde je prehliadač ešte podporovaný, nevydala v mesiaci november žiadne opravy kritických a závažných zraniteľností.

Odporúčania:

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

Zdroje:

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

Microsoft Edge

Spoločnosť Microsoft v mesiaci november opravila v prehliadači Microsoft Edge 2 závažné zraniteľnosti.

Závažné zraniteľnosti CVE-2023-36027 a CVE-2023-36024 môžu viesť k eskalácii privilégií. Útočník pre ich zneužitie musí presvedčiť obeť, aby interagovala s podvrhnutým škodlivým súborom.

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36027
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36024

Mozilla Firefox

V mesiaci november bolo opravených 6 vysoko závažných zraniteľností v línii Firefox a Firefox ESR.

Vysoko závažná zraniteľnosť CVE-2023-6204 dovoľuje pristupovať k pamäti mimo povolené hodnoty v komponente WebGL2.

Zraniteľnosti CVE-2023-6205 a CVE-2023-6207 umožňujú použiť dealokované miesto v pamäti v komponentoch MessagePort a ReadableByteStream.

CVE-2023-6206 týka nedostatočného oneskorenia aktivácie vyskakovacích okien a umožňuje zneužívanie kliknutia používateľa na spustenie akcie, ktorú nezamýšľal vykonať.

Zraniteľnosti CVE-2023-6212 (línia Firefox a Firefox ESR) a CVE-2023-6213 (línia Firefox) pokrývajú sadu zraniteľností ovplyvňujúcich bezpečnosť pamäte, ktoré môžu viesť ku poškodeniu pamäte alebo možnosti vykonávať kód.

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 120
Mozilla Firefox ESR verzie staršej ako 115.5

Odporúčania:

Odporúčame aktualizáciu Mozilla Firefox na verziu 120 a Mozilla Firefox ESR na verziu 115.5

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-50/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-49/

Google Chrome

V mesiaci november bola vydaná oprava 9 vysoko závažných zraniteľností prehliadača Google Chrome.

Zraniteľnosti CVE-2023-5996, CVE-2023-5997, CVE-2023-6112, CVE-2023-6346, CVE-2023-6347 a CVE-2023-6351 umožňujú použiť dealokované miesto pamäte v komponentoch WebAudio, Garbage Collection, Navigation, WebAudio, Mojo, , libavif.

CVE-2023-6348 sa týka nesprávnej manipulácie s dátovými typmi v komponente pre kontrolu pravopisu.

CVE-2023-6350 umožňuje pristupovať k pamäti mimo povolené hodnoty v komponente Libavif.

Aktívne zneužívaná zraniteľnosť CVE-2023-6345 súvisí s pretečením celočíselnej premennej v komponente Skia.

Zraniteľné systémy:

Google Chrome pre Windows verzie staršej ako 119.0.6045.199 /.200 a Linux a Mac verzie staršej ako 119.0.6045.199.

Odporúčania:

Odporúčame aktualizáciu prehliadača Chrome pre Windows aspoň na verziu 119.0.6045.199 /.200 a Linux a Mac aspoň na verziu 119.0.6045.199.

Zdroje:

https://chromereleases.googleblog.com/
https://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop_28.html
https://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop_14.html
https://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop.html

4. Adobe Acrobat a Reader

V produkte Adobe Acrobat a Reader bolo v mesiaci november opravených 9 vysoko závažných zraniteľností.

Zraniteľnosti CVE-2023-44336, CVE-2023-44359, CVE-2023-44367, CVE-2023-44371 a CVE-2023-44372 umožňujú použiť dealokované miesto v pamäti.

CVE-2023-44337, CVE-2023-44338 a CVE-2023-44366 umožňujú pristupovať mimo povolené hodnoty pamäte.

CVE-2023-44365 sa týka nesprávneho inicializovania adresy pamäte, resp. prístupu k neinicializovanému ukazovateľu.

Všetky závažné zraniteľnosti umožňujú ľubovoľné vykonávanie kódu.

Zraniteľné systémy:

Acrobat DC a Acrobat Reader DC pre Windows a Mac verzie 23.006.20360 a staršie,
Acrobat 2020 a Acrobat Reader 2020 pre Windows a Mac verzie 20.005.30524 a staršie.

Odporúčania:

Odporúčame aktualizáciu aspoň na verziu:
Acrobat DC a Acrobat Reader DC pre Windows a Mac 23.006.20380,
Acrobat 2020 a Acrobat Reader 2020 pre Windows a Mac 20.005.30539.

Zdroje:

https://helpx.adobe.com/security/security-bulletin.html
https://helpx.adobe.com/security/products/acrobat/apsb23-54.html

5. Frameworky

Microsoft .NET Framework

V mesiaci november spoločnosť Microsoft opravila 4 vysoko závažné zraniteľnosti vo frameworku .NET.

Zraniteľnosť CVE-2023-36038 sa nachádza v ASP.NET a umožňuje vyvolať nedostupnosť služby. To nastáva rušením HTTP požiadaviek na .NET 8 RC1, ktorý beží na IIS InProcess a vyčerpaním miesta v pamäti.

CVE-2023-36049 umožňuje zvýšenie oprávnení v systéme .NET. Útočník ju môže zneužiť zaslaním príkazov na FTP server.

Zraniteľnosti CVE-2023-36558 a CVE-2023-36560 sa nachádzajú v ASP.NET a umožňujú obchádzanie bezpečnostných prvkov.

Zraniteľné systémy:

.NET 6.0
.NET 7.0
ASP.NET Core 6.0
ASP.NET Core 7.0
Azure Identity SDK for .NET

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/en-us/security-guidance
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36038
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36049
https://nvd.nist.gov/vuln/detail/CVE-2023-36560
https://nvd.nist.gov/vuln/detail/CVE-2023-36558

Oracle Java

Veľká sada opráv je plánovaná na 16. januára 2024.

Zdroje:

https://www.oracle.com/security-alerts/

6. Iné závažné zraniteľnosti

Spoločnosti Intel a AMD opravili v balíku Microsoft Patch Tuesday viac ako 130 zraniteľností
Spoločnosti Intel a AMD vydali v novembri 2023 balík opráv pre procesory opravujúcich viac ako 130 zraniteľností. Zraniteľnosti sa týkajú chyby procesorov a umožňujú ľubovoľné vykonávanie kódu a eskaláciu privilégií. **Viac informácií na stránke.**

Zraniteľnosti aktívne zneužívané skupinami APT s napojením na Rusko a Čínu
Spoločnosť CISA vydala varovanie ohľadom aktívne zneužívaných bezpečnostných chýb v produktoch od Microsoft, Sophos a Oracle. Útoky boli zamerané na vládne organizácie v južnej Ázii a boli spojené so skupinou APT napojenou na Rusko a Čínu. **Viac informácií na stránke**.

Zero-day zraniteľnosť v Zimbra Collaboration
Zero-day zraniteľnosť CVE-2023-37580 je aktívne zneužívaná vo vládnych systémoch v Grécku, Moldavsku, Tunisku, Vietname a Pakistane na krádež emailových údajov, autentifikačných tokenov a prihlasovacích údajov. **Viac informácií na stránke.**

Zero-day zraniteľnosť v softvéri SysAid

Zero-day zraniteľnosť CVE-2023-47246 je aktívne zneužívaná v softvéri SysAid, čo umožňuje útočníkom nasadiť ransomvér Cl0p. Na zraniteľnosť poukázal bezpečnostný tím Profero. Úspešné zneužitie umožňuje útočníkom pristupovať k súborom a adresárom používateľov webového servera. **Viac informácií na stránke.**

Zero-day zraniteľnosti v Microsoft Exchange

Bezpečnostný expert, Piotr Bazydlo, spoločnosti Trend Micro Zero Day Initiative (ZDI) identifikoval štyri vysoko závažné zero-day zraniteľnosti na platforme Microsoft Exchange. Úspešné zneužitie umožňuje pristupovať k citlivým údajom a vzdialene vykonávať kód. **Viac informácií na stránke.**

Tri zero-day zraniteľnosti v softvéri Exim

Vývojársky tím Eximu vydal záplaty pre tri zero-day zraniteľností, na ktoré poukázala spoločnosť Trend Micro prostredníctvom Zero Day Initiative (ZDI). Úspešné zneužitie umožňuje vzdialené vykonávanie kódu na 3,5 milióna serveroch, ktoré by mohli byť ohrozené. **Viac informácií na stránke.**

Eskalácia oprávnení v systéme Linux

Spoločnosť Qualys objavila zraniteľnosť CVE-2023-4911, ktorá bola pomenovaná ako Looney Tunables. Úspešné zneužitie umožňuje útočníkovi získať oprávnenia na úrovni root a ovplyvňuje knižnicu GNU C (glibc) v operačnom systéme Linux. **Viac informácií na stránke.**

Zero-day zraniteľnosť v softvéri Citrix

Spoločnosť Citrix poukázala na dve vysoko závažné zraniteľnosti. Zero-day zraniteľnosť CVE-2023-4966 umožňuje obchádzanie viacfaktorovej autentifikácie a CVE-2023-4967 umožňuje vyvolanie nedostupnosti služby (DoS). Zraniteľnosti mohli byť zneužité na kyberšpionáž. **Viac informácií na stránke.**

Čínska kyberšpionáž v produktoch Atlassian

Spoločnosť Atlassian plánovane zruší podporu pre produkt Confluence Server. Po dátume 15. februára 2024 aktualizácie zabezpečenia, opravy chýb, technickú podporu a ani aktualizácie technického obsahu online pre produkty Server nebude poskytovať. Spoločnosť Microsoft poukázala na aktívne zneužívané zero-day zraniteľností hackerskou skupinou podporovanou čínskou vládou v produktoch Atlassian Confluence Data Center a Server. Úspešné zneužitie umožňuje zvýšiť privilégiá na administrátora, narušiť integritu a získať heslá používateľov. **Viac informácií na stránke.**