Mesačný prehľad kritických zraniteľností september 2023

1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci september 1 kritickú a 20 vysoko závažných zraniteľností.

Kritická zraniteľnosť CVE-2023-38148 sa nachádza v službe Internet Connection Sharing. Neautorizovanému útočníkovi dovoľuje vykonať kód odoslaním špeciálne vytvoreného paketu zraniteľnej službe Internet Connection Sharing.

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

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 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 Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- 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)

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-2023-38148
https://vuldb.com/?id.239590

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci september 15 vysoko závažných zraniteľností.

Zraniteľnosti vysokej závažnosti umožňujú vzdialené vykonávanie kódu a eskaláciu oprávnení. Zneužitie niektorých z nich môže viesť k úniku informácií a možnosti obchádzania bezpečnostných prvkov.

Zraniteľné systémy:

3D Builder
3D Viewer
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 2019 for Mac
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office LTSC for Mac 2021
Microsoft Office Online Server
Microsoft Outlook 2016 (32-bit edition)
Microsoft Outlook 2016 (64-bit edition)

Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 Service Pack 1 (64-bit editions)
Microsoft Word 2016 (32-bit edition)
Microsoft Word 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
https://msrc.microsoft.com/update-guide/

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 september 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 september opravila v prehliadači Microsoft Edge jednu závažnú zraniteľnosť.

Zraniteľnosť CVE-2023-36727 sa nachádza na webovom serveri a umožňuje podvrhnúť obeti podvodnú stránku. Pre úspešné zneužitie je potrebná interakcia zo strany obete so škodlivým URL odkazom.

Zraniteľné systémy:

Microsoft Edge (Chromium-based) build 117.0.2045.31.

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-2023-36727

Mozilla Firefox

V mesiaci september bola vydaná oprava 2 kritických a 6 vysoko závažných zraniteľností v línii Firefox.

Kritická zero-day zraniteľnosť CVE-2023-5217 sa nachádza v knižnici libvpx a súvisí s pretečením medzipamäte haldy. To môže viesť k vzdialenému vykonávaniu kódu. Zraniteľnosť sa týka formátu kódovania videa VP8.

Podobne kritická zraniteľnosť CVE-2023-4863 (predtým CVE-2023-5129) je chyba implementácie Huffmanovho kódovania vo formáte WebP v knižnici libwebp. Tiež bolo zaznamenané jej zneužívanie. Otvorením škodlivého obrázku formátu WebP môže dôjsť u pretečeniu medzipamäte na halde, čo môže útočníkovi umožniť vykonávanie kódu.

Zraniteľnosti CVE-2023-5168 a CVE-2023-5169 umožňujú zapisovať do pamäte mimo povolené hodnoty v komponentoch FilterNodeD2D1 a PathOps.

CVE-2023-5170, CVE-2023-5171 a CVE-2023-5172 umožňujú použiť dealokované miesto v pamäti v kompilátoroch Ion a Opm. Zneužitie CVE-2023-5170 môže viesť k úniku zo sandboxu prehliadača a CVE-2023-5172 k poškodeniu pamäte.

CVE-2023-5176 môže viesť k poškodeniu pamäte a vzdialenému vykonávaniu kódu v Firefox 117 Firefox ESR 115.2 a Thunderbird 115.2.

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 118.0.1
Mozilla Firefox ESR verzie staršej ako 115.3.1

Odporúčania:

Odporúčame aktualizáciu Mozilla Firefox na verziu 118.0.1 a Mozilla Firefox ESR na verziu 115.3.1

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-40/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-41/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-42/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-44/
https://www.helpnetsecurity.com/2023/09/27/cve-2023-5129/

Google Chrome

V mesiaci september bola vydaná oprava 7 vysoko závažných a 1 kritickej zraniteľnosti prehliadača Google Chrome.

Aktívne zneužívané zraniteľnosti CVE-2023-4863 a CVE-2023-5217 sa nachádzajú v knižniciach libwebp a libvpx a súvisia s pretečením medzipamäte haldy. Vysoko závažná zraniteľnosť CVE-2023-5217 sa týka formátu kódovania videa VP8 a kritická CVE-2023-4863 je chyba implementácie Huffmanovho kódovania vo formáte WebP.

Zraniteľnosť CVE-2023-4761 umožňuje pristupovať k pamäti mimo povolené hodnoty v komponente FedCM.

CVE-2023-4762 sa nachádza v komponente V8 a súvisí s neoverením typu premennej.

CVE-2023-4763 súvisí s použitím dealokovaného miesta pamäte v komponente Networks.

CVE-2023-4764 sa týka nesprávneho zabezpečenia používateľského rozhrania v mechanizme BFCache.

CVE-2023-5186 a CVE-2023-5187 umožňujú použiť dealokované miesto pamäte v komponentoch Passwords a Extensions.

Zraniteľné systémy:

Google Chrome pre Windows, Mac a Linux verzie staršej ako 117.0.5938.132.

Odporúčania:

Odporúčame aktualizáciu prehliadača Chrome pre Windows, Mac a Linux aspoň na verziu 117.0.5938.132.

Zdroje:

https://chromereleases.googleblog.com/2023/09/
https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html
https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_12.html
https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_27.html

4. Adobe Acrobat a Reader

V produkte Adobe Acrobat a Reader bola v mesiaci september opravená 1 vysoko závažná zraniteľnosť.

Zraniteľnosť CVE-2023-26369 umožňuje zapisovať do pamäte mimo povolené hodnoty a môže viesť k vykonávaniu ľubovoľného kódu. Pre zneužitie zraniteľnosti musí obeť otvoriť útočníkom podvrhnutý škodlivý súbor.

Zraniteľné systémy:

Acrobat DC a Acrobat Reader DC pre Windows a Mac verzie 23.003.20284 a staršie,
Acrobat 2020 a Acrobat Reader 2020 pre Windows 20.005.30514 a Mac verzie 20.005.30516 a staršie.

Odporúčania:

Odporúčame aktualizáciu aspoň na verziu:
Acrobat DC a Acrobat Reader DC pre Windows a Mac 23.006.20320,
Acrobat 2020 a Acrobat Reader 2020 pre Windows a Mac 20.005.30524.

Zdroje:

https://helpx.adobe.com/security/security-bulletin.html
https://helpx.adobe.com/security/products/acrobat/apsb23-34.html
https://nvd.nist.gov/vuln/detail/CVE-2023-26369

5. Frameworky

Microsoft .NET Framework

V mesiaci september spoločnosť Microsoft opravila 6 vysoko závažných zraniteľností vo frameworku .NET.

Zraniteľnosti vysokej závažnosti umožňujú vzdialené vykonávanie kódu. Zneužitie niektorých z nich môže viesť k narušeniu dostupnosti služby.

Zraniteľné systémy:

.NET 6.0
.NET 7.0
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.0 Service Pack 2
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.5 AND 4.7.2
Microsoft .NET Framework 3.5 AND 4.8
Microsoft .NET Framework 3.5 AND 4.8.1
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 4.6.2
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 4.8

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

Oracle Java

Veľká sada opráv je plánovaná na 17. októbra 2023.

Zdroje:

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

6. Iné závažné zraniteľnosti

Viacero zraniteľností v aplikácii Foxit PDF Editor a Reader

Spoločnosť Foxit Software vydala bezpečnostné aktualizácie pre Foxit PDF Editor pre platformy Windows a MacOS. Tieto aktualizácie opravujú niekoľko zraniteľností, ktoré môžu viesť k vzdialenému vykonávaniu kódu. Viac informácií na stránke.

Zraniteľnosť Microsoft Defender

Výskumníci poukázali na závažnú zraniteľnosť CVE-2023-24934, ktorá sa týka zneužitia aktualizačných procesov Windows Defender. Manipuláciou so súbormi v procese aktualizácie Defendera dokázali

ovplyvniť jeho fungovanie a spôsobiť zastavenie procesu pri neoprávnených zmenách. Zraniteľnosť môže viesť k zneužitiu systému pomocou vykonávania škodlivého kódu. Viac informácií na stránke.

Zraniteľnosť FortiOS umožňuje vykonávanie kódu

Spoločnosť Fortinet oznámila prítomnosť závažnej bezpečnostnej zraniteľnosti v produkte FortiOS. Zraniteľnosť umožňuje potenciálnemu útočníkovi vykonať na cieľovom zariadení ľubovoľný kód prostredníctvom špecificky vytvorených príkazov a môže viesť k celkovej kompromitácii zariadenia. Viac informácií na stránke.

Zraniteľnosť v sieťovom úložisku NAS od Western Digital a Synology

Spoločnosti Western Digital a Synology vydali varovanie pre sadu zraniteľností, ktoré môže ohroziť milióny zariadení NAS. Útočník by mohol využiť tieto chyby na krádež poverení, prístup k údajom používateľa a vzdialené, čím by získal kontrolu nad zariadením a možnosť vykonávania ďalších útokov. Viac informácií na stránke.

Viacero zraniteľností v operačnom systéme Junos OS

Spoločnosť Juniper Networks opravila viacero zraniteľností v komponente J-Web operačného systému Junos OS. Zreťazením týchto zraniteľností môže byť neautentifikovaný útočník schopný vykonávať kód na zariadeniach vzdialene. Spoločnosť Juniper Networks preto vydala výnimočnú bezpečnostnú aktualizáciu. Tieto zraniteľnosti postihujú všetky verzie operačného systému Junos OS na zariadeniach SRX a EX Series. Viac informácií na stránke.