# Mesačný prehľad kritických zraniteľností august 2023

## 1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci august 3 kritické a 32 vysoko závažných zraniteľností.

Kritické zraniteľnosti CVE-2023-35385, CVE-2023-36910 a CVE-2023-36911 a sa nachádzajú v službe Microsoft Message Queuing (MSMQ) a umožňujú vzdialené vykonávanie kódu (RCE). Pre ich zneužitie musí neautentifikovaný útočník odoslať zraniteľnému zariadeniu špeciálne vytvorený IP paket. Úspešné zneužitie zraniteľností umožňuje neautentifikovanému útočníkovi vzdialené vykonávanie kódu na cieľovom serveri.

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

### 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 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:

Na riešenie týchto zraniteľností by ste mali najprv skontrolovať, či je služba MSMQ aktuálne aktívna. Ak áno a nepoužívate ju, je nevyhnutné zastaviť jej prevádzku a zakázať jej spustenie. Následne by ste mali vytvoriť nové pravidlo pre Windows Firewall. Toto pravidlo s názvom „AUTOMOX WORKLET: Blokovať TCP 1801“ je navrhnuté na blokovanie akéhokoľvek prevádzky na TCP porte 1801.

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-2023-35385
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910

# 2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci august 3 kritické a 11 vysoko závažných zraniteľností.

Kritické zraniteľnosti CVE-2023-29328 a CVE-2023-29330 umožňujú útočníkovi vzdialené vykonávanie kódu v aplikácii Microsoft Teams a môžu spôsobiť nedostupnosť klienta. Na zneužitie týchto zraniteľností musí útočník presvedčiť obeť, aby sa pripojila k stretnutiu v aplikácii Teams. Pre úspešný útok nie sú potrebné špeciálne oprávnenia.

Zraniteľnosť CVE-2023-36895 sa nachádza v Microsoft Outlook a útočníkovi jej zneužitie umožní vzdialené vykonávanie kódu.

Vysoko závažné zraniteľnosti umožňujú vzdialené vykonávanie kódu, falšovanie a únik informácií.

## 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 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 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)
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Teams for Android
Microsoft Teams for Desktop
Microsoft Teams for iOS
Microsoft Teams for Mac
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)

### 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-2023-29328
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29330
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36895

## 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 august 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 august opravila v prehliadači Microsoft Edge jednu kritickú zraniteľnosť.

Zraniteľnosť CVE-2023-36741 sa nachádza v softvéri Chromium a umožňuje vzdialené vykonávanie kódu. Útočník potrebuje presvedčiť obeť, aby klikla na podvrhnutý odkaz a otvorila špeciálne vytvorený súbor.

### Zraniteľné systémy:

Microsoft Edge (Chromium-based) build 116.0.1938.62

### 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-2023-2033
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2033
https://cyberintell.blog/2023/08/31/microsoft-edge-faces-privilege-escalation-risk-with-cve-2023-36741/

## Mozilla Firefox

V mesiaci august bolo opravených 16 vysoko závažných zraniteľností v línii Firefox a Firefox ESR.

Zraniteľnosť CVE-2023-4573 sa týka prijímania údajov pre vykresľovanie cez mechanizmus IPC mStream.

Zraniteľnosti CVE-2023-4574 a CVE-2023-4575 sa týkajú vytvárania spätných volaní cez IPC pre zobrazenie okien Color Picker a File Picker.

CVE-2023-4576 súvisí s pretečením celočíselnej premennej vo funkcii RecordedSourceSurfaceCreation. Jej zneužitie by mohlo viesť k úniku z kontrolovaného prostredia (sandbox).

Zraniteľnosť CVE-2023-4577 sa týka funkcie UpdateRegExpStatics, ktorá by sa mohla pokúsiť pristúpiť k už odstránenému úložisku initialStringHeap. To môže viesť ku zneužiteľným podmienkam.

Zraniteľnosti CVE-2023-4056, CVE-2023-4057, CVE-2023-4058, CVE-2023-4584 a CVE-2023-4585 sa týkajú poškodenia pamäte a môžu viesť k vykonávaniu ľubovoľného kódu.

CVE-2023-4045 sa týka rozhrania Offscreen Canvas a umožňuje prístup k obrazovým informáciám z iného webu, ktorý je v rozpore s politikou same-origin.

CVE-2023-4046 sa týka zastaranej hodnoty pre globálnu premennú v analýze WASM JIT. Táto zraniteľnosť by mohla viesť k nesprávnej kompilácii a možnosti zneužitia pádu pri spracovaní obsahu.

CVE-2023-4047 umožňuje ukryť oznámenie o prepnutí do režimu plnej obrazovky využitím vyskakovacieho okna s výzvou. Útočník by chybu mohol zneužiť na zmätenie obete.

CVE-2023-4048 dovoľuje čítať mimo povolené hodnoty v pamäti pri spracovaní HTML pomocou komponentu DOMParser.

Úspešné zneužitie zraniteľnosti CVE-2023-4049 umožňuje útočníkovi využiť dealokované miesto v pamäti.

CVE-2023-4050 sa týka pretečenia vyrovnávacej pamäte zásobníka a mohlo viesť k úniku zo sandboxu.

Všetky tieto zraniteľnosti môžu viesť k zneužitiu dealokovaného miesta v pamäti po uvoľnení a spôsobiť pád systému.

### Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 117
Mozilla Firefox ESR verzie staršej ako 115.2

### Odporúčania:

Odporúčame aktualizáciu Mozilla Firefox na verziu 117 a Mozilla Firefox ESR na verziu 115.2

### Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-29/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-36/

## Google Chrome

V mesiaci august bola vydaná oprava 22 vysoko závažných zraniteľností prehliadača Google Chrome.

Zraniteľnosti CVE-2023-4068, CVE-2023-4069, CVE-2023-4070 a CVE-2023-4352 sú chyby zámeny typu premennej v komponente V8.

CVE-2023-4071, CVE-2023-4353 a CVE-2023-4354 súvisí s pretečením medzipamäte na halde v komponente Visuals, ANGLE a Skia.

Zraniteľnosti CVE-2023-4072, CVE-2023-4073, CVE-2023-4355, CVE-2023-4427 a CVE-2023-4428 v komponentoch WebGL, ANGLE, V8 a CSS dovoľujú čítať a zapisovať mimo povolené hodnoty v pamäti.

CVE-2023-4074, CVE-2023-4075, CVE-2023-4076, CVE-2023-2312, CVE-2023-4349, CVE-2023-4351, CVE-2023-4430, CVE-2023-4429 a CVE-2023-4572 umožňujú použiť dealokované miesto v pamäti v komponentoch Blink Task Scheduling, Cast, WebRTC, Offline, Device Trust Connectors, Network, Vulkan, Loader a MediaStream.

CVE-2023-4350 súvisí s nevhodnou implementáciou v komponente Fullscreen.

### Zraniteľné systémy:

Google Chrome pre Windows a Mac verzie staršej ako 116.0.5845.179/180 a Linux verzie staršej ako 116.0.5845.179.

### Odporúčania:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 116.0.5845.179/180 a Linux aspoň na verziu 116.0.5845.179.

### Zdroje:

https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_15.html
https://chromereleases.googleblog.com/2023/08/chrome-desktop-stable-update.html
https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_29.html

## 4. Adobe Acrobat a Reader

V produkte Adobe Acrobat a Reader bolo v mesiaci august opravených 16 kritických a 11 vysoko závažných zraniteľností.

Kritická zraniteľnosť CVE-2023-29320 umožňuje útočníkovi obísť bezpečnostné funkcie systému a kompromitovať zariadenie obete. Zraniteľnosť sa týka pretečenia vyrovnávacej pamäte zásobníka.

Kritické zraniteľnosti CVE-2023-38222, CVE-2023-38223, CVE-2023-38224, CVE-2023-38225, CVE-2023-38226, CVE-2023-38227, CVE-2023-38228, CVE-2023-38231, CVE-2023-38233, CVE-2023-38234 a CVE-2023-38246 umožňujú vykonávanie ľubovoľného kódu bez povolenia používateľa.

Kritické zraniteľnosti CVE-2023-38235, CVE-2023-38232, CVE-2023-38229 a CVE-2023-38230 môžu viesť k úniku údajov z pamäte a dovoľujú čítať mimo povolené hodnoty.

### Zraniteľné systémy:

Acrobat DC a Acrobat Reader DC pre Windows a Mac verzie 23.003.20244 a staršie,
Acrobat 2020 a Acrobat Reader 2020 pre Windows a Mac verzie 20.005.30467 a staršie.

### Odporúčania:

Odporúčame aktualizáciu aspoň na verziu:
Acrobat DC a Acrobat Reader DC pre Windows a Mac 23.003.20269,
Acrobat 2020 a Acrobat Reader 2020 pre Windows 20.005.30514.10514 a Mac 20.005.30516.10516

### Zdroje:

https://helpx.adobe.com/security/security-bulletin.html
https://helpx.adobe.com/security/products/acrobat/apsb23-30.html

## 5. Frameworky

## Microsoft .NET Framework

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

Zraniteľnosť CVE-2023-35390 bola nájdená pri použití určitých príkazov dotnet v adresároch so slabšími oprávneniami. To umožňuje vzdialené vykonávanie kódu.

Zraniteľnosť CVE-2023-35391 sa týka používania redis backplane v SignalR, čo môže viesť k odhaleniu informácií.

CVE-2023-36899 umožňuje zvýšenie oprávnení v systéme ASP.NET, zatiaľ čo CVE-2023-36873 sa týka falšovania.

Zraniteľnosť CVE-2023-38178 bola nájdená v komponente Kestrel a umožňuje klientovi obísť limit QUIC streamu v HTTP/3, čo spôsobuje odmietnutie služby.

CVE-2023-38180 sa týka nekontrolovanej spotreby zdrojov v komponente Kestrel a môže viesť k odmietnutiu služby.

### Zraniteľné systémy:

.NET 6.0
.NET 7.0
ASP.NET Core 2.1
Microsoft .NET Framework 2.0 Service Pack 2
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 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
https://nvd.nist.gov/vuln/detail/CVE-2023-35390
https://access.redhat.com/security/cve/cve-2023-35390
https://nvd.nist.gov/vuln/detail/CVE-2023-35391
https://access.redhat.com/security/cve/cve-2023-35391
https://nvd.nist.gov/vuln/detail/CVE-2023-36899
https://nvd.nist.gov/vuln/detail/CVE-2023-38178
https://access.redhat.com/security/cve/cve-2023-38178
https://nvd.nist.gov/vuln/detail/CVE-2023-38180
https://access.redhat.com/security/cve/cve-2023-38180

## Oracle Java

Najbližšia veľká sada opráv je plánovaná na 17.októbra 2023.

### Zdroje:

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

## 6. Iné závažné zraniteľnosti

***Zraniteľnosť v Joe Sandbox***

Spoločnosť Joe Security LLC po internom preskúmaní zistila vážnu zraniteľnosť vo svojom produkte Joe Sandbox. Zraniteľnosť sa nachádza v komponente dekompilácie .NET v knižnici tretej strany. Špeciálne vytvoreným škodlivým programom je možné vzdialene vykonať kód na serveri. Viac informácií na stránke.

***Kritická zraniteľnosť v routroch od spoločnosti MikroTik***

Spoločnosť VulnCheck poukázala na kritickú zraniteľnosť CVE-2023-30799, týkajúcu sa operačného systému MikroTik, RouterOS. Táto chyba dovoľuje útočníkom získať oprávnenia Super Admin a ohrozuje približne 500 000 až 900 000 systémov RouterOS, ktoré môžu byť napadnuté cez ich webové a/alebo Winbox rozhrania. na stránke.