MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ



OKTÓBER 2026

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci október 41 kritických a 1080 vysoko závažných zraniteľností v operačných systémoch Windows.

V ovládači **Windows Reliable Multicast Transport Driver (RMCAST)** sa vyskytuje kritická zraniteľnosť CVE-2026-69789 umožňujúca neautorizovanému útočníkovi **vykonávať kód** z priľahlej siete. Chyba zabezpečenia vyplýva z pretečenia vyrovnávacej pamäte na halde. Útočník pre jej zneužitie potrebuje poznať konfiguráciu systému.

Kritická zraniteľnosť CVE-2026-69802 komponentu **Network Device Enrollment Service (NDES)** súvisí so slabým mechanizmom autentifikácie. Neautorizovaný útočník jej zneužitím získa schopnosť **vzdialene vykonávať kód**.

Ovládač **Microsoft PostScript Printer Driver** obsahuje tri kritické zraniteľnosti. CVE-2026-70147 a CVE-2026-70153 umožňujú neautorizovanému útočníkovi **vzdialene vykonávať kód**. Zraniteľnosť CVE-2026-108467 vyžaduje pre zneužitie nízke oprávnenia. Chyby zabezpečenia vyplývajú z pretečenia vyrovnávacej pamäte na halde. Útočník pre ich zneužitie môže poslať špeciálne vytvorenú požiadavku na tlač alebo paket.

Kritická zraniteľnosť sa nachádza aj v komponente **Windows Remote Desktop Gateway Service**. CVE-2026-70187 umožňuje použiť dealokované miesto v pamäti. Zraniteľnosť môže zneužiť neautorizovaný útočník so znalosťou systému na **vzdialené vykonanie kódu**. Potrebuje k tomu poslať zraniteľnému systému špeciálne vytvorený paket.

Zraniteľnosť komponentu **Windows Active Directory Domain Services** dovoľuje neautorizovanému útočníkovi **vzdialené vykonávanie kódu** zaslaním špeciálne vytvoreného paketu. CVE-2026-70229 vyplýva z nevhodného autorizačného mechanizmu. Útočník potrebuje poznať zraniteľný systém.

Dve kritické zraniteľnosti v **Active Directory Federation Services (AD FS)** umožňujú neautorizovaným vzdialeným útočníkom **vykonávať spoofingové útoky**. CVE-2026-96222 a CVE-2026-108131 vyplývajú z nevhodnej validácie certifikátov.

Päť kritických zraniteľností sa nachádza v komponente **Windows DHCP Server**. Neautorizovanému útočníkovi umožňujú **vzdialené vykonávanie kódu** zaslaním špeciálne vytvoreného paketu zraniteľnej službe. CVE-2026-88117, CVE-2026-88119, CVE-2026-88120 a CVE-2026-96934 umožňujú opätovne použiť dealokované miesto v pamäti. CVE-2026-88171 súvisí s dvojitým uvoľnením pamäte. Všetky okrem CVE-2026-96934 pre úspešné zneužitie vyžadujú, aby útočník vyhral súbeh procesov.

Kritickú zraniteľnosť obsahuje aj služba **Windows DHCP Client**. Chyba zabezpečenia CVE-2026-70250 súvisí so vznikom súbehu procesov a možnosťou opätovného použitia dealokovanej pamäte. Neautorizovanému útočníkovi umožňuje **vykonávať kód** z priľahlej siete.

Windows ALPC obsahuje kritickú zraniteľnosť CVE-2026-83917, ktorá dovoľuje lokálnemu útočníkovi s nízkymi oprávneniami, ktorý vyhrá súbeh procesov, **eskalovať svoje oprávnenia až na úroveň SYSTEM**. Súvisí s možnosťou opätovného použitia dealokovanej pamäte.

V komponente **Windows GDI+** sa vyskytuje kritická zraniteľnosť CVE-2026-83934 umožňujúca neautorizovanému útočníkovi **vzdialene vykonávať kód**. Chyba zabezpečenia vyplýva z pretečenia vyrovnávacej pamäte na halde. Útočník pre jej zneužitie potrebuje presvedčiť obeť, aby otvorila špeciálne vytvorený súbor.

Windows Graphics obsahuje kritické zraniteľnosti v súčastiach **Kernel** a **Component**. CVE-2026-88073 v Kernel dovoľuje lokálnemu útočníkovi s nízkymi oprávneniami použiť dealokované miesto v pamäti a **eskalovať oprávnenia na úroveň SYSTEM**. CVE-2026-100215 v Component umožňuje lokálnemu útočníkovi bez oprávnení **lokálne vykonávať kód** s oprávneniami prihláseného používateľa. Na to potrebuje presvedčiť obeť, aby otvorila špeciálne vytvorený súbor alebo navštívila webstránku obsahujúcu špeciálne vytvorené vnorené fonty OpenType.

Komponent **Windows Virtualization-Based Security (VBS)** obsahuje päť kritických zraniteľností, ktoré umožňujú lokálnym útočníkom s nízkymi oprávneniami **eskalovať svoje privilégiá na úroveň SYSTEM**. CVE-2026-88074 súvisí s pretečením celočíselnej premennej. CVE-2026-96914 súvisí s pretečením celočíselnej premennej a medzipamäte na halde. CVE-2026-102211 vzniká kvôli možnosti použitia dealokovanej pamäte a vzniku súbehu, ktorý musí útočník vyhrať pre jej úspešné zneužitie. CVE-2026-108130 spôsobuje pretečenie medzipamäte na halde. CVE-2026-108471 súvisí s nekompletným zoznamom nepovolených vstupov.

Kritická zraniteľnosť CVE-2026-88174 komponentu **Windows Deployment Services** umožňujú útočníkom bez oprávnení **vzdialene vykonávať kód**. Súvisí s nesprávnym manažmentov zdrojov a vznikom súbehu procesov.

V komponente **Windows Raw Image Extension** sa nachádzajú dve kritické zraniteľnosti, ktoré umožňujú neautorizovanému útočníkovi **vzdialene vykonávať kód**. CVE-2026-96202 súvisí s pretečením vyrovnávacej pamäte na halde. Pre jej zneužitie potrebuje útočník presvedčiť obeť, aby otvorila špeciálne vytvorený súbor formátu RAW. Chyba zabezpečenia CVE-2026-96943 súvisí s pretečením celočíselnej premennej a vyrovnávacej pamäte na halde. Pre jej zneužitie potrebuje útočník presvedčiť obeť, aby pristúpila ku zložke obsahujúce špeciálne

vytvorený súbor formátu RAW. Zraniteľnosť je možné zneužiť pri generovaní thumbnailu alebo náhľadu súboru.

Komponente **Windows Kernel** má kritickú zraniteľnosť CVE-2026-96913, ktorá súvisí s pretečením vyrovnávacej pamäte na halde. Lokálnemu útočníkovi s nízkymi oprávneniami dovoľuje **eskalovať svoje privilégiá na úroveň SYSTEM**.

Kritická zraniteľnosť sa nachádza aj v komponente **Microsoft Windows Media Foundation**. CVE-2026-96952 súvisí s pretečením vyrovnávacej pamäte na halde. Zraniteľnosť môže zneužiť neautorizovaný útočník na **vzdialené vykonanie kódu**. Potrebuje k tomu presvedčiť obeť, aby otvorila špeciálne vytvorený súbor.

Podobnú zraniteľnosť obsahuje **Windows Media Video Decoder**. CVE-2026-100220 súvisí s pretečením vyrovnávacej pamäte na halde. Zraniteľnosť môže zneužiť neautorizovaný útočník na **vzdialené vykonanie kódu**. Potrebuje k tomu presvedčiť obeť, aby otvorila špeciálne vytvorený súbor.

Dve kritické zraniteľnosti komponentu **Windows Text Shaping** dovoľujú neautorizovanému útočníkovi **vzdialené vykonávanie kódu**. CVE-2026-97814 vyplýva z pretečenia vyrovnávacej pamäte na halde a zneužiť ju možno zaslaním špeciálne vytvoreného paketu zraniteľnej inštancii. CVE-2026-102225 umožňuje čítanie pamäte mimo povolené hodnoty a súvisí aj s chybou pri orezávaní číselných hodnôt. Útočník pre jej zneužitie potrebuje presvedčiť obeť, aby otvorila špeciálne vytvorený súbor.

Kritická zraniteľnosť CVE-2026-108460 komponentu **Windows Message Queuing** umožňuje použiť dealokované miesto v pamäti. Pre jej zneužitie potrebuje neautorizovaný útočník poslať špeciálne vytvorený paket zraniteľnej službe a vyhrať súbeh, čo mu umožní **vzdialené vykonanie kódu**. Komponent **Windows Message Queuing Queue Manager** obsahuje chybu zabezpečenia CVE-2026-100202, vyplývajúcu z možnosti opätovného použitia dealokovaného miesta v pamäti. Neautorizovaný útočník získa schopnosť **vzdialeného vykonania kódu**, keď pošle špeciálne vytvorenú správu zraniteľnej službe.

Dve kritické zraniteľnosti komponentu **Microsoft QUIC** dovoľujú neautentifikovanému útočníkovi **vzdialené vykonávanie kódu**. CVE-2026-100219 vyplýva z možnosti opätovného použitia dealokovaného miesta v pamäti. CVE-2026-105016 súvisí s pretečením vyrovnávacej pamäte na halde. Zneužiť ich možno zaslaním špeciálne vytvoreného paketu zraniteľnej inštancii.

Windows Hyper-V obsahuje tri kritické zraniteľnosti. CVE-2026-105733 súvisí s nesprávnou inicializáciou zdrojov a lokálnemu útočníkovi s nízkymi oprávneniami umožňuje **vykonávanie kódu**. Útočník ju môže zneužiť na únik z vnoreného virtuálneho stroja a získanie administrátorských oprávnení na hostiteľskom virtuálnom stroji. Chyba zabezpečenia CVE-2026-108399 vyplýva z pretečenia vyrovnávacej pamäte na halde a lokálnemu útočníkovi s vysokými oprávneniami umožňuje **navýšiť svoje oprávnenia** na hostiteľskom systéme.

Kritická zraniteľnosť CVE-2026-108400 v komponente **HEVC Video Extensions** súvisí s pretečením celočíselnej premennej. Neautorizovanému útočníkovi dovoľuje **vzdialene vykonávať kód**. Útočník pre jej zneužitie potrebuje presvedčiť obeť, aby otvorila špeciálne vytvorený súbor.

V komponente **Microsoft Windows PDF** sa nachádza kritická zraniteľnosť CVE-2026-108457, ktorá umožňuje neautorizovanému útočníkovi sa znalosťou zraniteľného systému **vzdialené vykonávanie kódu**. Zraniteľnosť vyplýva z možnosti zapisovania do pamäte mimo povolené hodnoty. Útočník ju môže zneužiť zaslaním špeciálne vytvorenej prílohy e-mailu zraniteľnému systému, ktorý automaticky spracúva súbory PDF.

Zraniteľnosti vysokej závažnosti možno zneužiť na **eskaláciu privilégií**, **vzdialené vykonávanie kódu**, **zneprístupnenie služby (DoS)**, **získanie prístupu k citlivým informáciám**, **spoofingové útoky**, **zásahy do systémov** a **odchádzanie bezpečnostných prvkov**.

ZRANITEĽNÉ SYSTÉMY:

- HEVC Video Extensions
- HEVC Video Extensions for Licensed Applications
- HEVC Video Extensions from Device Manufacturer
- Microsoft Configuration Manager 2509
- Microsoft Configuration Manager 2603
- MPEG-2 Video Extension
- Raw Image Extension
- 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 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 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 25H2 for ARM64-based Systems

- Windows 11 Version 25H2 for x64-based Systems
- Windows 11 Version 26H1 for ARM64-based Systems
- Windows 11 version 26H1 for x64-based Systems
- Windows 11 Version 26H2 for ARM64-based Systems
- Windows 11 Version 26H2 for x64-based Systems
- Windows Security App
- 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 2025
- Windows Server 2025 (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-2026-100202
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-100215
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-100219
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-100220
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-102211
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-102214
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-102225
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-105016
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-105733
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108130

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108131
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108399
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108400
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108457
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108460
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108467
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108471
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69789
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69802
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70147
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70153
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70187
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70229
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70250
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83917
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83934
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-88073
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-88074
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-88117
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-88119
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-88120
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-88171
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-88174
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96202
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96222
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96913
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96914
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96934
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96943
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96952
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97814

Koniec podpory pre Windows 10, staršie verzie Windows 11 a Windows Server 2016

Spoločnosť Microsoft v roku 2025 plánovane ukončila podporu pre všetky verzie Windows 10. Po dátume 14. októbra 2025 už tieto produkty nedostávajú aktualizácie zabezpečenia, aktualizácie nesúvisiace so zabezpečením, opravy chýb, technickú podporu a ani aktualizácie technického obsahu online. **Po rokovaní s organizáciou Euroconsumers však v Európskom hospodárskom priestore predĺžila spoločnosť Microsoft bezplatnú podporu systémov Windows 10 o rok, teda do 13. októbra 2026. Podmienkou môže byť prihlásenie sa cez Microsoft account.**

Pre Windows 11 Microsoft plánovane ukončí podporu pre v súčasnosti podporované verzie nasledovne:

23H2 Enterprise a Education: Podpora skončí 10. novembra 2026.
24H2 Home a Pro: Podpora **skončila** 13. októbra 2026.
24H2 Enterprise a Education: Podpora skončí 12. októbra 2027.

Spoločnosť Microsoft ďalej plánuje ukončiť podporu pre Windows Server 2016 ku dňu 12. januára 2027.

ODPORÚČANIA:

Administrátorom a používateľom systému Windows 10 odporúčame prejsť na novšiu verziu operačného systému alebo používať rozšírenie ESU (Extended Security Updates), ktoré je potrebné zakúpiť si samostatne. **Viac informácií na stránke výrobcu.**

Administrátorom a používateľom verzií systému Windows 11 s končiacou podporou odporúčame prejsť na najnovšiu verziu operačného systému, t.j. 26H2.

2. KANCELÁRSKE BALÍKY MICROSOFT OFFICE A OFFICE WEB APPS

Spoločnosť Microsoft vydala v mesiaci október bezpečnostné aktualizácie, ktoré opravujú 39 kritických a 183 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Štyri kritické zraniteľnosti boli opravené v **Microsoft Office PowerPoint**. Neautorizovaný útočník ich môže zneužiť na **vzdialené vykonávanie kódu**. Zraniteľnosti CVE-2026-70215 a CVE-2026-88144 vyplývajú z možnosti opätovného použitia dealokovaného miesta v pamäti a CVE-2026-88207 súvisí s pretečením vyrovnávacej pamäte haldy. Pre ich zneužitie musí útočník presvedčiť obeť, aby otvorila špeciálne pripravený súbor MS Office. Zraniteľnosť CVE-2026-88178 vyplýva

z možnosti opätovného použitia dealokovaného miesta v pamäti a pre jej zneužitie nie je potrebná interakcia obete. Útočným vektorom pre všetky chyby zabezpečenia môže byť aj náhľad dokumentu (Preview Pane).

V **Microsoft Outlook** bolo opravených šesť kritických zraniteľností. Neautorizovaným útočníkom umožňujú **vzdialené vykonávanie kódu**. CVE-2026-70242, CVE-2026-70291, CVE-2026-97016 a CVE-2026-108448 sú spôsobené pretečením vyrovnávacej pamäte na halde. CVE-2026-88156 súvisí s pretečením vyrovnávacej pamäte na zásobníku. CVE-2026-97749 vyplýva z dvojitého uvoľnenia pamäte. Všetky okrem CVE-2026-108448 je možné zneužiť zaslaním špeciálne vytvoreného e-mailu obeti. Pre jej vyvolanie stačí, keď obeť zobrazí e-mail v Outlook Reading Pane. Pre zneužitie CVE-2026-70291, CVE-2026-108448 a CVE-2026-88156 postačuje vygenerovanie náhľadu škodlivého e-mailu (Preview Pane).

V **Microsoft Word** bolo opravených päť kritických zraniteľností, ktoré môže neautorizovaný útočník zneužiť na **vzdialené vykonávanie kódu**. CVE-2026-70269 je spôsobená pretečením vyrovnávacej pamäte na halde a pretečením celočíselnej premennej. Jej zneužitie vyžaduje znalosť cieľového systému, no útočným vektorom môže byť aj náhľad dokumentu (Preview Pane). CVE-2026-70300 vzniká kvôli neošetrenej dereferencii nedôveryhodného ukazovateľa. Zneužiť ju možno zaslaním špeciálne vytvoreného dokumentu WordPerfekt s prelinkovaným grafickým súborom. Ku jej zneužitiu dochádza pri spracovaní dokumentu vo Word Reading Pane. Vektorom útoku však môže byť aj náhľad dokumentu (Preview Pane). CVE-2026-88185 a CVE-2026-108439 vyplývajú z pretečenia vyrovnávacej pamäte na halde. Vektorom útoku pre ne môže byť aj náhľad dokumentu (Preview Pane). Druhú z nich dokáže útočník zneužiť zaslaním špeciálne vytvoreného súboru RTF, ktorý obeť otvorí alebo zobrazí jeho náhľad. Posledná chyba zabezpečenia s identifikátorom CVE-2026-108440 je spôsobená pretečením vyrovnávacej pamäte na zásobníku a zneužiť ju možno zaslaním špeciálne vytvoreného súboru RTF, ktorý obeť otvorí alebo zobrazí jeho náhľad (Preview Pane).

Dvadsať kritických zraniteľností bolo opravených v aplikácii **Microsoft Excel**. Neautorizovaný útočník ich môže zneužiť na **vzdialené vykonanie kódu**. Pre ich zneužitie však potrebuje interakciu obete. Náhľad dokumentu (Preview Pane) nie je možným vektorom zneužitia týchto zraniteľností. Chyby CVE-2026-97739 a CVE-2026-97753 vyplývajú z pretečenia celočíselnej premennej a vyrovnávacej pamäte na halde. Zraniteľnosti CVE-2026-97741, CVE-2026-97756, CVE-2026-97758, CVE-2026-97765, CVE-2026-97776, CVE-2026-97780, CVE-2026-100210 a CVE-2026-102855 sú spôsobené pretečením vyrovnávacej pamäte na halde. CVE-2026-97742 a CVE-2026-97761 vznikajú kvôli pretečeniu vyrovnávacej pamäte na zásobníku. CVE-2026-97745, CVE-2026-97759, CVE-2026-100209 a CVE-2026-100211 spôsobuje možnosť opätovného použitia dealokovanej pamäte. Chyby zabezpečenia CVE-2026-97755 a CVE-2026-105718 súvisia s možnosťou čítania pamäte mimo povolené hodnoty a nevhodným ošetrením vstupov. CVE-2026-97767 vzniká kvôli neošetrenej dereferencii nulového ukazovateľa a dvojitému uvoľneniu pamäte. Posledná chyba zabezpečenia, CVE-2026-97778, súvisí s pretečením celočíselnej premennej.

V aplikáciách **Microsoft Office Visio** boli opravené dve kritické zraniteľnosti. CVE-2026-102856 súvisí s pretečením celočíselnej premennej a vyrovnávacej pamäte na halde. CVE-2026-102857

vzniká kvôli pretečeniu vyrovnávacej pamäte na halde a chybe vo výpočte o 1. Neautorizovaný útočník ich môže zneužiť na **vzdialené vykonanie kódu**. Pre ich zneužitie však potrebuje interakciu obete. Náhľad dokumentu (Preview Pane) nie je možným vektorom zneužitia týchto zraniteľností.

Microsoft Sharepoint obsahuje kritickú zraniteľnosť, ktorá umožňuje vzdialeným neautorizovaným útočníkom **navýšenie svojich oprávnení**. Zraniteľnosť CVE-2026-102866 je spôsobená nevhodnou verifikáciou kryptografických podpisov. Ak útočník získa platný overovací token obete, môže ho modifikovať a poslať zraniteľnému serveru, čím sa autentifikuje ako obeť. Náhľad dokumentu (Preview Pane) nie je možným útočným vektorom.

Aplikácia **Microsoft Bookings** obsahuje kritickú zraniteľnosť CVE-2026-94510, ktorá umožňuje vzdialenému neautentifikovanému útočníkovi **eskalovať svoje oprávnenia**. Vyplýva z možnosti obídenia autorizácie kvôli kľúčom, ktoré kontroluje používateľ. Pre jej zneužitie útočník nepotrebuje interakciu obete. Spoločnosť Microsoft chybu zabezpečenia opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre jej odstránenie.

Vysoko závažné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu**, **navýšenie privilégií**, **získavanie citlivých informácií**, **obídenie bezpečnostných prvkov, zásahy do systémov** a **spoofingové útoky**.

ZRANITEĽNÉ SYSTÉMY:

- Azure DevOps CLI Extension
- azure_security_keyvault_certificates (Rust)
- azure_security_keyvault_keys (Rust)
- azure_security_keyvault_secrets (Rust)
- azure-keyvault-administration
- azure-keyvault-certificates
- azure-keyvault-keys
- azure-keyvault-secrets
- azure-keyvault-securitydomain
- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft Bookings
- Microsoft Office 365 for Mac
- Microsoft Office for Android

- Microsoft Office LTSC 2021 for 32-bit editions
- Microsoft Office LTSC 2021 for 64-bit editions
- Microsoft Office LTSC 2024 for 32-bit editions
- Microsoft Office LTSC 2024 for 64-bit editions
- Microsoft Office LTSC for Mac 2021
- Microsoft Office LTSC for Mac 2024
- Microsoft Paint
- Microsoft Power Apps for Android
- Microsoft PowerToys
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription Edition
- Office Online Server
- Outlook.com
- Skype for Business Server 2015 CU13
- Skype for Business Server 2019 CU8
- Skype for Business Server Subscription Edition CU1

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-2026-100209
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-100210
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-100211
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-102855
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-102856
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-102857

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-102866
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-105718
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108439
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108440
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108448
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70215
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70242
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70269
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70291
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70300
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-88144
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-88156
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-88178
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-88185
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-88207
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-94510
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97016
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97739
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97741
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97742
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97745
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97749
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97753
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97755
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97756
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97758
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97759
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97761
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97765
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97767
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97776

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97778
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-97780

Koniec podpory pre Office 2021

Spoločnosť Microsoft v 13. októbra 2026 plánovane ukončila podporu pre Office 2021. Po tomto dátume už tento balík nedostáva aktualizácie zabezpečenia, aktualizácie nesúvisiace so zabezpečením, opravy chýb, technickú podporu a ani aktualizácie technického obsahu online.

ODPORÚČANIA:

Administrátorom a používateľom balíkov Office 2016 a Office 2019 odporúčame prejsť na novšiu verziu (Office 2024), cloudovú verziu Office 365 alebo používať Office LTSC. **Viac informácií na** stránke výrobcu.

3. INTERNETOVÉ PREHLIADAČE

MICROSOFT EDGE

Spoločnosť Microsoft v mesiaci október opravila jednu kritickú a 15 vysoko závažných zraniteľností vo webovom prehliadači Microsoft Edge.

Kritická zraniteľnosť CVE-2026-96202 umožňuje neautorizovanému útočníkovi **vzdialene vykonávať kód**. súvisí s pretečením vyrovnávacej pamäte na halde. Pre jej zneužitie potrebuje útočník presvedčiť obeť, aby otvorila špeciálne vytvorený súbor formátu RAW.

Vysoko závažné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu**, **navýšenie privilégií**, **získavanie citlivých informácií** a **obídenie bezpečnostných prvkov**.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft Edge (Chromium-based) verzie staršie ako 156.0.4314.50

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-2026-96202

MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci október opravila 141 vysoko závažných zraniteľností v líniách internetových prehliadačov Firefox, Firefox ESR, Firefox for iOS a Firefox for Android.

Firefox for iOS obsahuje zraniteľnosť CVE-2026-103418 v komponente Translation Services, ktorá umožňuje **vykonávať útoky typu XSS**. Dôvodom je priame preberanie jazykových atribútov z HTML kódu webstránok, čo dovoľuje obchádzať politiku Content Security Policy a **vykonávať kód**.

Línie Firefox a Firefox ESR obsahujú vysoko závažnú zraniteľnosť CVE-2026-109704 v komponente Application Update, ktorá umožňuje **eskalovať oprávnenia**.

Línie Firefox a Firefox ESR obsahujú 7 vysoko závažných zraniteľností v komponente Networking. CVE-2026-109705 vyplýva z nesprávne stanovených hraničných podmienok, súvisí s možnosťou opätovného použitia dealokovanej pamäte a dovoľuje **únik zo sandboxu** prehliadača. CVE-2026-109707 kvôli možnosti opätovného použitia dealokovanej pamäte umožňuje **únik zo sandboxu**. CVE-2026-109708 vyplýva z nesprávne stanovených hraničných podmienok a umožňuje **únik zo sandboxu**. CVE-2026-117862 vyplýva z nesprávne stanovených hraničných podmienok a umožňuje **eskalovať oprávnenia**. CVE-2026-117884 a CVE-2026-117907 umožňujú opätovne použiť dealokovanú pamäť. CVE-2026-117952 súvisí s neinicializovanou pamäťou.

Zraniteľnosť CVE-2026-117899 komponentu Networking: HTTP sa nachádza v líniách Firefox a Firefox ESR. Súvisí s možnosťou opätovného použitia dealokovanej pamäte.

Zraniteľnosť CVE-2026-117922 komponentu Networking: WebSockets v líniách Firefox a Firefox ESR vyplýva z možnosti opätovného použitia dealokovanej pamäte.

Chyba zabezpečenia CVE-2026-117868 línií Firefox a Firefox ESR v komponente DOM: Networking umožňuje **únik zo sanboxu**.

Chyby zabezpečenia CVE-2026-109717, CVE-2026-117930 a CVE-2026-117935 línií Firefox a Firefox ESR v komponente DOM: Bindings (WebIDL) dovoľujú opätovne použiť dealokovanú pamäť.

Komponent DOM: Core & HTML obsahuje 21 vysoko závažných zraniteľností. CVE-2026-109724, CVE-2026-109725, CVE-2026-117869, CVE-2026-117881, CVE-2026-117887, CVE-2026-117895, CVE-2026-117896, CVE-2026-117901, CVE-2026-117919, CVE-2026-117925, CVE-

2026-117929, CVE-2026-117932, CVE-2026-117936, CVE-2026-117940, CVE-2026-117943, CVE-2026-117949, CVE-2026-117951, CVE-2026-117953, CVE-2026-118015, CVE-2026-118016 umožňujú opätovné použitie dealokovanej pamäte. CVE-2026-117950 súvisí s nesprávne stanovenými hraničnými podmienkami. Chyby zabezpečenia sú prítomné v líniách Firefox, aj Firefox ESR, okrem CVE-2026-118015 a CVE-2026-118015, ktoré zasahujú iba líniu Firefox.

Línie Firefox a Firefox ESR obsahujú vysoko závažnú zraniteľnosť CVE-2026-109728 v komponente DOM: Animation, ktorá umožňuje opätovné použitie dealokovanej pamäte. Línia Firefox obsahuje zraniteľnosť CVE-2026-118012, ktorá tak isto umožňuje opätovné použitie dealokovanej pamäte.

Línie Firefox a Firefox ESR obsahujú vysoko závažnú zraniteľnosť CVE-2026-109732 v komponente DOM: Streams, ktorá dovoľuje opätovné použitie dealokovanej pamäte.

Línie Firefox a Firefox ESR obsahujú tri vysoko závažné zraniteľnosti v komponente DOM: Navigation. CVE-2026-117860 umožňuje **obísť politiku Same-origin**. Zneužitie CVE-2026-117861 môže viesť ku **úniku zo sanboxu**. CVE-2026-118008 v línii Firefox dovoľuje **eskalovať oprávnenia** útočníka.

Chyby zabezpečenia CVE-2026-117883 a CVE-2026-117920 línií Firefox a Firefox ESR v komponente DOM: HTML Parser umožňujú opätovné použitie dealokovanej pamäte.

Chyby zabezpečenia CVE-2026-117900 a CVE-2026-117931 línií Firefox a Firefox ESR v komponente DOM: Editor dovoľujú opätovne použiť dealokovanú pamäť.

Línie Firefox a Firefox ESR obsahujú vysoko závažnú zraniteľnosť CVE-2026-117941 v komponente DOM: CSS Object Model, ktorá umožňuje opätovne použiť dealokovanú pamäť.

Tri chyby zabezpečenia sa nachádzajú v komponente Graphics línií Firefox a Firefox ESR. Zraniteľnosť CVE-2026-109712 umožňuje **uniknúť zo sanboxu** kvôli neinicializovanej pamäti. Chyba zabezpečenia s označením CVE-2026-109730 súvisí s pretečením celočíselnej premennej. Chyba CVE-2026-117871 súvisí s neplatným ukazovateľom.

Zraniteľnosť CVE-2026-109710 komponentu Graphics: Text v líniách Firefox a Firefox ESR vyplýva z možnosti opätovného použitia dealokovanej pamäte. CVE-2026-118009 v línii Firefox okrem možnosti opätovného použitia dealokovanej pamäte súvisí s pretečením celočíselnej premennej. CVE-2026-117886 vyplýva nesprávne stanovených hraničných podmienok. Obsahujú ju obe produktové línie.

Komponent Graphics: Canvas2D v líniách Firefox a Firefox ESR obsahuje päť vysoko závažných zraniteľností. Zraniteľnosti CVE-2026-109711, CVE-2026-117918 a CVE-2026-117866 vyplývajú z možnosti opätovného použitia dealokovanej pamäte, pričom posledná z nich umožňuje **eskalovať oprávnenia**. CVE-2026-109731 súvisí s nesprávne stanovenými hraničnými podmienkami. CVE-2026-117888 súvisí s neinicializovanou pamäťou.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť CVE-2026-109719 v komponente Graphics: CanvasWebGL. Chyba zabezpečenia vyplýva zo vzniku súbehu a možnosti opätovného použitia dealokovanej pamäte.

Línie Firefox a Firefox ESR obsahujú vysoko závažnú zraniteľnosť v komponente Graphics: ImageLib. Chyby zabezpečenia CVE-2026-117908 vyplýva z možnosti opätovného použitia dealokovanej pamäte.

Línie Firefox a Firefox ESR obsahujú v komponente Graphics: WebRender zraniteľnosť CVE-2026-117917, ktorá súvisí s neplatným ukazovateľom.

V komponente WebRTC: Networking sa nachádza vysoko závažná zraniteľnosť CVE-2026-117892, ktorá súvisí s možnosťou opätovného použitia dealokovanej pamäte a dovoľuje **únik zo sandboxu**. Zasahuje línie Firefox a Firefox ESR.

WebRTC: Signaling obsahuje tri zraniteľnosti. CVE-2026-118005 a CVE-2026-118006 v línii Firefox súvisia s možnosťou opätovného použitia dealokovanej pamäte, pričom druhá umožňuje **eskaláciu oprávnení**. CVE-2026-117894 v líniách Firefox a Firefox ESR vyplýva z nesprávne stanovených hraničných podmienok.

Chyby zabezpečenia CVE-2026-109706 a CVE-2026-117878 sa nachádzajú v línii Firefox a Firefox ESR v komponente Storage: IndexedDB. Umožňujú opätovné použitie dealokovanej pamäte.

Línie Firefox a Firefox ESR obsahujú vysoko závažnú zraniteľnosť CVE-2026-109709 v komponente Security: Process Sandboxing, ktorá umožňuje **eskaláciu oprávnení** vedie k **úniku informácií**.

Zraniteľnosť komponentu Security: PSM v líniách Firefox a Firefox ESR s označením CVE-2026-117893 vyplýva z nesprávne stanovených hraničných podmienok.

V komponente Crash Reporting sa nachádza vysoko závažná zraniteľnosť CVE-2026-109713, ktorá dovoľuje opätovné použitie dealokovanej pamäte. Zasahuje línie Firefox a Firefox ESR.

Línia Firefox obsahuje vysoko závažnú zraniteľnosť CVE-2026-109714 v komponente Layout, ktorá vyplýva z nesprávne stanovených hraničných podmienok. Firefox a Firefox ESR obsahujú aj ďalších 5 chýb zabezpečenia CVE-2026-117867, CVE-2026-117882, CVE-2026-117934, CVE-2026-117938 a CVE-2026-117944, ktoré umožňujú opätovné použitie dealokovanej pamäte.

V komponente Layout: Text and Fonts v líniách Firefox a Firefox ESR sa nachádzajú štyri vysoko závažné zraniteľnosti. Zraniteľnosť CVE-2026-109723 súvisí s pretečením celočíselnej premennej. Zraniteľnosti CVE-2026-117876, CVE-2026-117877 a CVE-2026-117902 umožňujú opätovné použitie dealokovanej pamäte.

Zraniteľnosť CVE-2026-117875 komponentu Layout: Scrolling and Overflow umožňuje opätovné použitie dealokovanej pamäte. Nachádza sa v líniách Firefox a Firefox ESR.

Línie Firefox a Firefox ESR obsahujú vysoko závažné zraniteľnosti CVE-2026-117879 a CVE-2026-117897 v komponente Layout: Tables, ktoré vyplývajú z nesprávne stanovených hraničných podmienok.

Zraniteľnosť CVE-2026-117885 komponentu Layout: Grid umožňuje opätovné použitie dealokovanej pamäte. Nachádza sa v líniách Firefox a Firefox ESR.

Línie Firefox a Firefox ESR obsahujú vysoko závažnú zraniteľnosť CVE-2026-117915 v komponente Layout: Block and Inline, ktorá vyplýva z nesprávne stanovených hraničných podmienok.

Zraniteľnosť CVE-2026-118013 komponentu Layout: Images, Video, and HTML Frames umožňuje opätovné použitie dealokovanej pamäte. Nachádza sa v línii Firefox.

Podobná vysoko závažná zraniteľnosť sa nachádza v komponente Layout: Positioned pre Firefox a Firefox ESR. Chyba s označením CVE-2026-118013 umožňuje opätovné použitie dealokovanej pamäte.

V komponente JavaScript Engine sa nachádza 7 vysoko závažných zraniteľností. CVE-2026-109715, CVE-2026-109716, CVE-2026-117889 a CVE-2026-117946 vyplývajú z nesprávne stanovených hraničných podmienok. CVE-2026-117870 umožňuje opätovné použitie dealokovanej pamäte. CVE-2026-117910 a CVE-2026-117937 súvisia s neplatným ukazovateľom. Zasahujú línie Firefox a Firefox ESR.

Osem vysoko závažných zraniteľností zasahuje komponent JavaScript Engine: JIT pre obe produktové línie Firefox a jedna pre líniu Firefox. CVE-2026-109721 a CVE-2026-117942 súvisia s nesprávne stanovenými hraničnými podmienkami. CVE-2026-109722, CVE-2026-109733 a CVE-2026-117890 vyplývajú z chybnej kompilácie v nástroji JIT. CVE-2026-109729, CVE-2026-117891 a CVE-2026-117898 umožňujú opätovné použitie dealokovanej pamäte. Zraniteľnosť CVE-2026-118014 zasahujúca líniu Firefox dovoľuje opätovné použitie dealokovanej pamäte.

V komponente JavaScript: WebAssembly sa nachádza vysoko závažná zraniteľnosť CVE-2026-109720. Súvisí s chybnou kompiláciou v nástroji JIT.

Štyri vysoko závažné zraniteľnosti v komponente JavaScript: GC dovoľujú opätovné použitie dealokovanej pamäte. Zraniteľnosti CVE-2026-117865, CVE-2026-117904 a CVE-2026-117909 zasahujúce línie Firefox a Firefox ESR. CVE-2026-118007 zasahuje líniu Firefox.

Komponent JavaScript: Standard Library zasahuje vysoko závažná zraniteľnosť CVE-2026-117872, ktorá dovoľuje opätovné použitie dealokovanej pamäte. Zasahuje línie Firefox a Firefox ESR.

Línie Firefox a Firefox ESR obsahujú päť vysoko závažných zraniteľností v komponente XML. CVE-2026-109718, CVE-2026-117880, CVE-2026-117939 a CVE-2026-117947 dovoľujú opätovné

použitie dealokovanej pamäte. CVE-2026-117945 súvisí s nesprávne stanovenými hraničnými podmienkami.

V komponente SVG sa nachádza osem vysoko závažných zraniteľností. Línie Firefox a Firefox ESR obsahujú vysoko závažné zraniteľnosti CVE-2026-109726, CVE-2026-117913, CVE-2026-117914, CVE-2026-117927 a CVE-2026-117948 ktoré dovoľujú opätovné použitie dealokovanej pamäte. CVE-2026-117926 vyplýva z nesprávne definovaných hraničných podmienok. Chyby zabezpečenia CVE-2026-113399 a CVE-2026-118017 zasahujú iba líniu Firefox. Prvá súvisí s nesprávne stanovenými hraničnými podmienkami a druhá dovoľuje opätovné použitie dealokovanej pamäte.

Línie Firefox a Firefox ESR obsahujú päť zraniteľností v komponente Audio/Video. Chyby zabezpečenia CVE-2026-109727, CVE-2026-117903 a CVE-2026-117923 súvisia s možnosťou opätovného použitia dealokovanej pamäte. Zraniteľnosť CVE-2026-117863 súvisí s neinicializovanou pamäťou a môže viesť k **úniku informácií**. Chyba CVE-2026-117873 vzniká kvôli nesprávne stanoveným hraničným podmienkam.

Vysoko závažné zraniteľnosti CVE-2026-117905 a CVE-2026-117911 komponentu Audio/Video: Playback v líniách Firefox a Firefox ESR vznikajú kvôli možnosti opätovného použitia dealokovanej pamäte.

Produktové línie Firefox, Firefox ESR a Firefox for Android obsahujú vysoko závažnú zraniteľnosť CVE-2026-113470. Nachádza sa v komponente Security Block-lists, Allow-lists, and other State a jedná sa o kryptografickú zraniteľnosť spojenú s **kompromitovaným certifikátom** eMudhra.

Chyba zabezpečenia CVE-2026-117864 umožňuje **uniknúť zo sanboxu**. Zasahuje komponent Form Manager línií Firefox a Firefox ESR.

Línie Firefox a Firefox ESR obsahujú vysoko závažnú zraniteľnosť CVE-2026-117874 v komponente Internationalization, ktorá dovoľuje opätovné použitie dealokovanej pamäte.

Podobne zraniteľnosti CVE-2026-117906 a CVE-2026-117921 v komponente CSS Parsing and Computation línií Firefox a Firefox ESR umožňujú opätovné použitie dealokovanej pamäte. CVE-2026-117912 a CVE-2026-117928 umožňujú obísť politiku Same-origin. CVE-2026-117933 a CVE-2026-118011 dovoľujú útoky typu Frame poisoning, resp. manipuláciu s prvkami iframe. Prvá zasahuje obe produktové línie, druhá iba líniu Firefox.

Línie Firefox a Firefox ESR obsahujú vysoko závažné zraniteľnosti CVE-2026-117916 a CVE-2026-117924 v komponente XSLT, ktoré dovoľujú opätovné použitie dealokovanej pamäte.

Línia Firefox ESR obsahuje vysoko závažnú zraniteľnosť CVE-2026-118010 v komponente Disability Access APIs, ktorá umožňuje opätovné použitie dealokovanej pamäte.

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox verzie staršej ako 159
- Mozilla Firefox ESR verzie staršej ako 115.44 a 153.6
- Firefox for Android verzie staršej ako 158.0.2
- Firefox for iOS verzie staršej ako 157.1

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 159 a Firefox ESR na verziu 115.44 alebo 153.6. Firefox for Android aktualizujte na 158.0.2 a Firefox for iOS aspoň na 157.1.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-105/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-106/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-107/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-108/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-111/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-112/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-113/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-116/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-118/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-119/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-120/

GOOGLE CHROME

V mesiaci október spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 25 kritických a 222 vysoko závažných zraniteľností.

Komponent Accessibility obsahuje kritické zraniteľnosti CVE-2026-113279 a CVE-2026-113271, ktoré umožňujú opätovné použitie dealokovanej pamäte.

Komponent ANGLE obsahuje kritickú zraniteľnosť, ktorá vyplýva z pretečenia nešpecifikovanej vyrovnávacej pamäte. Chyba zabezpečenia dostala identifikátor CVE-2026-110152.

Komponent Browser obsahuje kritické zraniteľnosti CVE-2026-106197 a CVE-2026-110149, ktoré umožňujú opätovné použitie dealokovanej pamäte.

Komponent Core obsahuje kritickú zraniteľnosť CVE-2026-110165, ktorá umožňuje opätovné použitie dealokovanej pamäte.

Rovnako v komponente CSS sa nachádza kritická zraniteľnosť CVE-2026-113072, ktorá umožňuje opätovné použitie dealokovanej pamäte.

Chybu zabezpečenia umožňujúcu opätovné použitie dealokovanej pamäte obsahuje tiež komponent FileAPI. Dostala označenie CVE-2026-118331.

Chyba zabezpečenia CVE-2026-118306 umožňuje opätovné použitie dealokovanej pamäte. Obsahuje ju komponent FileSystem.

Komponent Chromecast obsahuje kritickú zraniteľnosť CVE-2026-106382, ktorá umožňuje opätovné použitie dealokovanej pamäte.

Chyba zabezpečenia CVE-2026-118344 umožňuje opätovné použitie dealokovanej pamäte. Obsahuje ju komponent Layout.

Chybu zabezpečenia umožňujúcu opätovné použitie dealokovanej pamäte obsahuje tiež komponent Media. Dostala označenie CVE-2026-110151.

Rovnako v komponente MediaStream sa nachádza kritická zraniteľnosť CVE-2026-76024, ktorá umožňuje opätovné použitie dealokovanej pamäte.

Komponent Navigation obsahuje kritickú zraniteľnosť CVE-2026-106358, ktorá umožňuje opätovné použitie dealokovanej pamäte.

Chyba zabezpečenia CVE-2026-110161 umožňuje opätovné použitie dealokovanej pamäte. Obsahuje ju komponent Network.

Komponent Paint obsahuje kritickú zraniteľnosť CVE-2026-113280, ktorá umožňuje opätovné použitie dealokovanej pamäte.

Komponent PDF obsahuje kritickú zraniteľnosť CVE-2026-110136, ktorá umožňuje opätovné použitie dealokovanej pamäte.

Chybu zabezpečenia umožňujúcu opätovné použitie dealokovanej pamäte obsahuje tiež komponent Prerender. Dostala označenie CVE-2026-110922.

Dve kritické chyby zabezpečenia sa nachádzajú v komponente **Skia**. CVE-2026-113341 umožňuje opätovné použitie dealokovanej pamäte. CVE-2026-118348 vzniká kvôli pretečeniu celočíselnej premennej.

Opätovné použitie dealokovanej pamäte umožňuje aj kritická zraniteľnosť CVE-2026-110148 komponentu **SVG**.

Kritická chyba zabezpečenia v komponente **Track** umožňuje opätovné použitie dealokovanej pamäte. Dostala identifikátor CVE-2026-106347.

Dve kritické zraniteľností boli opravené v komponente **WebGL**. Chyby zabezpečenia CVE-2026-120931 a CVE-2026-103628 dovoľujú zápis do pamäte mimo povolené hodnoty.

Komponent **WebRTC** obsahuje kritickú zraniteľnosť CVE-2026-113303, ktorá umožňuje opätovné použitie dealokovanej pamäte.

Spoločnosť Google opravila vysoko závažné zraniteľnosti v komponentoch **Accessibility, ANGLE, Animation, Autofill, Bindings, Blink, Bluetooth, Browser, Cache, CacheStorage, Canvas, Command, Compositing, Contextual Tasks, Core, CustomTabs, Date, Dawn, Desktop, DevTools, DisplayLocking, DOM, Editing, Extensions, FedCM, FileSystem, Focus, Fonts, Forms, Frames, GarbageCollection, GPU, Headless, HTML, Chrome Tabs, Chrome for iOS, ImageCapture, Input, Installer, Media, MediaStream, Metrics, Modularization, Mojo, Navigation, Network, Omnibox, Paint, Parser, Passwords, Payments, PDF, PDFium, PictureInPicture, Privacy, Proxy, Proxy Auth, Quota, ReadingList, ReadingMode, Select, ServiceWorker, ShapeDetection, SiteIsolation, Skia, Storage, SVG, TabStrip, ThirdParty, Tint, Transactions Platform, Translate, Turbolev, UI, Updater, V8, Video, Views, WebAppInstalls, WebAudio, WebGL, WebRTC, WebUI, WTF, XML**. Tieto dovoľujú čítať a zapisovať do pamäte mimo povolené hodnoty, použiť dealokovanú pamäť a neinicializované zdroje, súvisia s pretečením medzipamäte či celočíselnej premennej, vyplývajú zo zámeny typu premennej, vzniku súbehu procesov, nedostatočnej validácie nedôveryhodných vstupov. Súvisia s chybami pamäte, autorizácie a zobrazenia, validácie certifikátov, rozpoznávania referencií, čistenia pamäte a validácie stavu. Umožňujú získavať citlivé informácie, eskalovať oprávnenia.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows verzie staršej ako 156.0.8078.79/.80
- Google Chrome pre Mac verzie staršej ako 156.0.8078.79/.80
- Google Chrome pre Linux verzie staršej ako 156.0.8078.79

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows aspoň na verziu 156.0.8078.79/.80, Mac aspoň na verziu 156.0.8078.79/.80 a Linux aspoň na verziu 156.0.8078.79.

ZDROJE:

- https://chromereleases.googleblog.com/2026/10
- https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_086471744.html
- https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html
- https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01886704284.html
- https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html
- https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_0562499947.html
- https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02107719452.html

4. ADOBE ACROBAT A READER

V mesiaci október spoločnosť Adobe neopravila žiadne kritické ani vysoko závažné zraniteľnosti v produktoch Adobe Acrobat a Reader.

ZDROJE:

- https://helpx.adobe.com/security.html#acrobat

5. FRAMEWORKY

MICROSOFT .NET FRAMEWORK

V mesiaci október spoločnosť Microsoft opravila 2 kritické a 35 vysoko závažných zraniteľností vo frameworku .NET.

Kritická zraniteľnosť CVE-2026-96222 v Active Directory Federation Services (AD FS) zasahuje tiež produkty Microsoft .NET. Vyplýva z nevhodnej validácie certifikátov. Neautorizovaným vzdialeným útočníkom umožňuje vykonávať **spoofingové útoky**.

Komponent Microsoft QUIC obsahuje kritickú zraniteľnosť, ktorá dovoľuje neautentifikovanému útočníkovi **vzdialené vykonávanie kódu**. CVE-2026-105016 súvisí s pretečením vyrovnávacej pamäte na halde. Zneužiť ju možno zaslaním špeciálne vytvoreného paketu zraniteľnej inštancii.

Vysoko závažné zraniteľnosti spočívajú okrem iného v nedostatočnej kontrole a ochrane vstupov a dát, nesprávne implementovaným autorizačným mechanizmom a v nesprávnej implementácii kontroly pôvodu dát/komunikácie. Vyplývajú zo zámeny typu premennej, možnosti zápisu do pamäte mimo povolené hodnoty. Súvisia so súbehom procesov, nevhodným a neefektívnym prideľovaním zdrojov a nevhodným narábaním s nedôveryhodnými dátami. Väčšinu z nich môže zneužiť vzdialený útočník bez oprávnení. Umožňujú mu **navýšiť svoje oprávnenia, vzdialene vykonávať kód, získať prístup k citlivým informáciám, spôsobiť nedostupnosť služby (DoS), obchádzať bezpečnostné prvky** a **zasahovať do systémov**.

ZRANITEĽNÉ SYSTÉMY:

- .NET 10.0 installed on Linux
- .NET 10.0 installed on Mac OS
- .NET 10.0 installed on Windows
- .NET 10.0 runtime installed on Linux
- .NET 10.0 runtime installed on Mac OS
- .NET 10.0 runtime installed on Windows
- .NET 11.0 installed on Linux
- .NET 11.0 installed on Mac OS
- .NET 11.0 installed on Windows
- .NET 11.0 runtime installed on Linux
- .NET 11.0 runtime installed on Mac OS

- .NET 11.0 runtime installed on Windows
- .NET 8.0 installed on Linux
- .NET 8.0 installed on Mac OS
- .NET 8.0 installed on Windows
- .NET 8.0 runtime installed on Linux
- .NET 8.0 runtime installed on Mac OS
- .NET 8.0 runtime installed on Windows
- .NET 9.0 installed on Linux
- .NET 9.0 installed on Mac OS
- .NET 9.0 installed on Windows
- .NET 9.0 runtime installed on Linux
- .NET 9.0 runtime installed on Mac OS
- .NET 9.0 runtime installed on Windows
- .NET source-build Linux tarballs (all archive types)
- ASP.NET Core 10.0
- ASP.NET Core 11.0
- ASP.NET Core 8.0
- ASP.NET Core 9.0
- ASP.NET Core runtime and targeting-pack Linux tarballs (Microsoft-published)
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2
- 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 4.6.2/4.7/4.7.1/4.7.2
- Microsoft .NET Framework 4.8
- Microsoft .NET Framework 4.8.1

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 vyhľadávača.

ZDROJE:

- https://msrc.microsoft.com/update-guide/en-us
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96222
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-105016

ORACLE JAVA

Spoločnosť Oracle v mesiaci október vydala bezpečnostné aktualizácie, ktoré opravujú jednu kritickú a 3 vysoko závažné zraniteľnosti v rámci Oracle Java SE.

Kritická zraniteľnosť CVE-2026-91403 sa nachádza v komponente JSSE. Vzdialený neautentifikovaný útočník ju môže zneužiť pomocou webových služieb, z ktorých sa dodávajú dáta do API rozhraní. Získa tak **prístup k súborom, ktoré môže čítať, modifikovať a mazať**. Môže na to využiť viaceré protokoly. Zraniteľné sú tiež sandboxované nasadenia aplikácií Java Web Start a appletov Java, ktoré vykonávajú nedôveryhodný kód a využívajú Java sandbox.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2026-91484 sa nachádza v komponente Java plugin. Lokálny útočník s nízkymi oprávneniami by ju mohol zneužiť pre získanie možnosti **pristupovať, vytvárať, modifikovať a mazať údaje**, vrátane kritických dát.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2026-43660 sa nachádza v komponente JavaFX (WebKitGTK). Neautentifikovaný vzdialený útočník by ju mohol zneužiť pomocou viacerých protokolov pre **získanie kontroly nad zraniteľnou inštanciou Java SE a JavaFX**. Na to potrebuje získať súčinnosť obete.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2026-91415 sa nachádza v komponente 2D. Zneužiť ju môže neautentifikovaný vzdialený útočník pomocou viacerých protokolov. Získa tak schopnosť spôsobiť **mrznutie alebo pád zraniteľnej inštancie (DoS)** a môže **získať prístup ku časti dát** prístupných pre inštanciu.

ZRANITEĽNÉ SYSTÉMY:

- Oracle Java SE: 8u503, 8u503-perf, 11.0.32.1, 17.0.20.1, 21.0.12.1, 25.0.4.1, 27
- Oracle JavaFX: 21.0.12, 25.0.4, 27

- Oracle GraalVM for JDK: 17.0.20.1, 21.0.12.1
- GraalVM Enterprise Edition: 21.3.19.1.1

ODPORÚČANIA:

Odporúčame aktualizovať zraniteľné verzie Java SE na aktuálne verzie prostredníctvom Java Auto Update alebo postupu na stránke spoločnosti Oracle.

ZDROJE:

- https://www.oracle.com/security-alerts/
- https://www.oracle.com/security-alerts/cpuoct2026.html#AppendixJAVA
- https://www.oracle.com/security-alerts/cpuoct2026verbose.html#JAVA
- https://csirt.sk/posts/4183.html

INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

AKTÍVNE ZNEUŽÍVANÉ KRITICKÉ ZRANITEĽNOSTI CITRIX NETSCALER

Vývojári platformy Citrix upozornili na dve kritické zraniteľnosti v produktoch NetScaler ADC a NetScaler Gateway, ktoré umožňujú vzdialenému neautentifikovanému útočníkovi vykonať ľubovoľný kód na zariadení. Spoločnosť Citrix potvrdila aktívne zneužívanie týchto zraniteľností v reálnych útokoch. Viac informácií na stránke.

Vývojári spoločnosti Citrix vydali tiež aktualizácie opravujúce aktívne zneužívanú vysoko závažnú zraniteľnosť v systémoch Citrix NetScaler ADC a Citrix NetScaler Gateway. Jej úspešným zneužitím môže vzdialený útočník spôsobiť nedostupnosť služby (DoS). Viac informácií na stránke.

ZRANITEĽNOSŤ PRODUKTOV ATLASSIAN AKTÍVNE ZNEUŽÍVANÁ

Spoločnosť Atlassian opravila aktívne zneužívanú kritickú zraniteľnosť v produktoch Jira Software, Jira Service Management Data Center, Confluence Data Center, Bitbucket Data Center, Bamboo Data Center, Crowd Data Center, Crucible a Fisheye. Zraniteľnosť umožňuje vzdialenému neautentifikovanému útočníkovi čítať ľubovoľné súbory v koreňovom adresári aplikácie, pokiaľ pozná ich názov a súborovú cestu. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI CISCO LICENSE ON-PREM (SSM ON-PREM)

Spoločnosť Cisco vydala bezpečnostné aktualizácie pre Cisco License On-Prem (predtým Smart Software Manager On-Prem), ktoré opravujú interne objavené tri kritické a jednu vysoko závažnú zraniteľnosť. Zraniteľnosti umožňujú vzdialene injektovať kód, pristupovať bez autentifikácie ku kritickým funkciám, či citlivým informáciám. Viac informácií na stránke.

CISCO OPRAVILA KRITICKÉ ZRANITEĽNOSTI V APIC

Spoločnosť Cisco vydala bezpečnostné aktualizácie pre Cisco Application Policy Infrastructure Controller (APIC), ktoré opravujú interne objavené kritické zraniteľnosti. Tri kritické zraniteľnosti súvisia s chybami v narábaní s rôznymi zdrojmi v rámci ich životného cyklu, nevhodným spôsobom neutralizácie nebezpečných prvkov a nesprávnym riadením prístupov. Viac informácií na stránke.

CISCO SECURE EMAIL GATEWAY MÁ AKTÍVNE ZNEUŽÍVANÚ KRITICKÚ ZRANITEĽNOSŤ

Spoločnosť Cisco opravila kritickú aktívne zneužívanú zraniteľnosť vo funkcii Advanced Malware Protection produktu Cisco Secure Email Gateway, ktorá neautentifikovanému vzdialenému útočníkovi umožňuje prostredníctvom e-mailu so špeciálne upravenou prílohou zapisovať ľubovoľné súbory a vykonávať príkazy s oprávneniami používateľa root. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ SPLUNK ENTERPRISE UMOŽŇUJE VYKONÁVAŤ PRÍKAZY OS

Vývojári spoločnosti Splunk opravili kritickú zraniteľnosť v produkte Splunk Enterprise, pri ktorej chýbajúca autentifikácia v rozhraní Patroni REST API umožňuje neautentifikovanému útočníkovi so sieťovým prístupom k členovi clustra „search head“ vykonať ľubovoľné príkazy OS. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI NGINX UMOŽŇUJÚ SPÔSOBIŤ NEDOSTUPNOSŤ SLUŽBY

Spoločnosť F5 opravila 3 kritické zraniteľnosti v NGINX Plus a NGINX Open Source, ktorých zneužitím môže vzdialený neautentifikovaný útočník prostredníctvom špeciálne upravených HTTP požiadaviek spôsobiť nedostupnosť služby (DoS) a pri vypnutej ochrane ASLR alebo jej úspešnom obídení môže získať schopnosť vykonávať kód. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI MARIADB

Vývojári databázového servera MariaDB opravili tri kritické zraniteľnosti, ktoré súvisia s chybami jeho komponentov pri narábaní s pamäťou a s obchádzaním moderného kódovania názvov tabuliek a súborov. Vzdialenému útočníkovi s nízkymi oprávneniami umožňujú vykonávať kód, spôsobiť nedostupnosť služby a získavať či meniť dáta. Viac informácií na stránke.

ORACLE OPRAVILA 1295 ZRANITEĽNOSTÍ

Spoločnosť Oracle vydala októbrovú aktualizáciu Critical Patch Update, ktorá obsahuje 1 295 bezpečnostných záplat v 129 produktoch, vrátane opráv 89 kritických zraniteľností. Šesť z nich dosiahlo maximálne skóre CVSS 10,0. Mnohé kritické zraniteľnosti môže útočník zneužiť na diaľku, bez potreby autentifikácie. Viac informácií na stránke.

PHP MÁ DVE KRITICKÉ ZERO-DAY ZRANITEĽNOSTI

Vývojári jazyka PHP vydali opravy dvoch kritických zraniteľností, ktoré umožňujú neautentifikované vzdialené vykonávanie ľubovoľného kódu na zraniteľnom serveri. Stručná informácia o zraniteľnostiach unikla na verejnosť pred vydaním opravných aktualizácií. Viac informácií na stránke.

V NODE.JS OPRAVILI DESAŤ ZRANITEĽNOSTÍ

Vývojári Node.js vydali bezpečnostné aktualizácie opravujúce desať zraniteľností, z ktorých najzávažnejšia sa nachádza v dekodéri kompresnej knižnice Brotli. Kritická zraniteľnosť umožňuje neautentifikovanému útočníkovi prostredníctvom špeciálne vytvorených komprimovaných údajov vyvolať poškodenie pamäte, znefunkčniť službu, získať prístup ku citlivým informáciám alebo potenciálne vzdialene vykonávať kód. Viac informácií na stránke.

ZERO-DAY ZRANITEĽNOSTI JADRA LINUXU

Na verejných mailing listoch pre Linux kernel boli zverejnené technické informácie viacerých ešte neopravených zraniteľností linuxového jadra. Ku šiestim z nich boli zverejnené stručné informácie. Útočníkom umožňujú vzdialene vykonávať kód, lokálne eskalovať svoje oprávnenia a získať prístup k citlivých informáciám. Najzávažnejšie zraniteľnosti sa nachádzajú v implementácii protokolu SMB. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ TCP V JADRE LINUX UMOŽŇUJE VYKONÁVAŤ PRÍKAZY

Vývojári jadra operačného systému Linux opravili kritickú zraniteľnosť, ktorá dovoľuje vzdialenému neautentifikovanému útočníkovi vykonávať na zraniteľnom serveri príkazy s oprávneniami používateľa root. Viac informácií na stránke.

ZRANITEĽNOSŤ DNS RESOLVERA BIND VEDIE K NEDOSTUPNOSTI SLUŽBY

Vývojári BIND, softvéru pre implementáciu protokolu DNS, opravili vysoko závažnú zraniteľnosť, ktorá umožňuje vzdialenému neautorizovanému útočníkovi spôsobiť vyčerpanie zdrojov servera a jeho nedostupnosť. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ FORTISANDBOX

Spoločnosť Fortinet opravila kritickú zraniteľnosť v nástroji FortiSandbox, ktorá umožňuje vzdialenému neautentifikovanému útočníkovi obísť prihlásenie do grafickej konzoly. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI WASMTIME VEDÚ K ÚNIKU ZO SANDBOXU

Vývojári runtime prostredia Wasmtime opravili dve kritické zraniteľnosti v kompilátore Cranelift, ktoré umožňujú vzdialenému útočníkovi s kontrolou nad kódom, ktorý vstupuje do procesu, spôsobiť nežiaduce správanie kódu a uniknúť zo sandboxu Wasm. Viac informácií na stránke.

VO VEEAM BACKUP & REPLICATION OPRAVILI ŠTYRI ZRANITEĽNOSTI

Vývojári zálohovacieho nástroja Veeam Backup & Replication vydali opravy štyroch zraniteľností. Jedna je hodnotená ako kritická, jedna vysoko závažná a dve stredne závažné. Útočníkom umožňujú obísť autorizáciu, získať vysoké oprávnenia a zapisovať súbory na ľubovoľné miesto na zálohovacom serveri. Viac informácií na stránke.