

MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

SEPTEMBER 2026



CSIRT.SK



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

1. OPERAČNÉ SYSTÉMY MICROSOFT WINDOWS

Spoločnosť Microsoft opravila v mesiaci september 78 kritických a 649 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritická zraniteľnosť CVE-2026-58599 v knižnici **Microsoft Windows Codecs Library** sa nachádza vo funkcionalite pre narábanie so súbormi formátu HEVC. Vyplýva z pretečenia vyrovnávacej pamäte na halde. Neautorizovaný lokálny útočník ju môže zneužiť na **vykonanie kódu**.

Kritická zraniteľnosť CVE-2026-65669 sa nachádza v komponente **Microsoft SQL Server**. Súvisí s nevhodným spôsobom neutralizácie špeciálnych prvkov. Neautorizovaný vzdialený útočník ju môže zneužiť a **eskalovať svoje oprávnenia**. Na to potrebuje interakciu obeť.

Šesť kritických zraniteľností komponentu **Windows Imaging Component** dovoľuje neautorizovanému útočníkovi **vzdialené vykonávanie kódu**. CVE-2026-70296 umožňuje zapisovanie do pamäte mimo povolené hodnoty a ako jediná nevyžaduje interakciu obeť. CVE-2026-69499 vyplýva z pretečenia celočíselnej premennej. CVE-2026-69860, CVE-2026-73013, CVE-2026-7302 a CVE-2026-77495 vyplývajú z pretečenia vyrovnávacej pamäte na halde.

Päť kritických zraniteľností sa nachádza v komponente **Windows Secure Kernel Mode**. Lokálnemu autorizovanému útočníkovi umožňuje **eskaláciu svojich oprávnení**, bez potreby interakcie obeť. CVE-2026-69501 a CVE-2026-83939 súvisia s dereferenciou nedôveryhodného ukazovateľa, pričom prvá ako jediná vyžaduje pre jej úspešné zneužitie iba nízke oprávnenia. CVE-2026-69906 vyplýva z pretečenia vyrovnávacej pamäte na halde, CVE-2026-69846 z pretečenia celočíselnej premennej a CVE-2026-85921 súvisí s dvojitým uvoľnením pamäte.

Kritická zraniteľnosť sa nachádza aj v komponente **Windows Remote Desktop**. CVE-2026-69518 súvisí s pretečením vyrovnávacej pamäte na halde. Zraniteľnosť môže zneužiť neautorizovaný útočník na **vzdialené vykonanie kódu**. Potrebuje k tomu presvedčiť obeť, aby sa pripojila k jeho relácii a prijala od neho špeciálne vytvorené dáta z clipboardu.

V ovládači **Windows Reliable Multicast Transport Driver (RMCAST)** sa vyskytujú tri kritické zraniteľnosti umožňujúce neautorizovanému útočníkovi **vzdialene vykonávať kód** zaslaním

špeciálne vytvoreného paketu zraniteľnej služby. Všetky súvisia s možnosťou opätovného použitia dealokovaného miesta v pamäti.

Kritická zraniteľnosť CVE-2026-69579 komponentu **Windows Message Queuing** umožňuje použiť dealokované miesto v pamäti. Pre jej zneužitie potrebuje neautorizovaný útočník poslať špeciálne vytvorený paket zraniteľnej služby, čo mu umožní **vzdialené vykonanie kódu**.

V komponente **Windows Routing and Remote Access Service (RRAS)** sa nachádzajú štyri kritické zraniteľnosti, ktoré umožňujú **vzdialené vykonávanie kódu**. Zraniteľnosti CVE-2026-69590, CVE-2026-69852, CVE-2026-72950 a CVE-2026-72959 vyplývajú z pretečenia vyrovnávacej pamäte na halde. Prvá z nich nevyžaduje od útočníka žiadne oprávnenia, ostatné vyžadujú nízke oprávnenia.

Tri kritické zraniteľnosti v ovládači **Windows Services for NFS ONCRPC XDR** umožňujú použiť dealokované miesto v pamäti a vedú k možnosti **vykonávať kód**. Zraniteľnosti CVE-2026-69595 a CVE-2026-78445 môže zneužiť a vzdialený neautorizovaný útočník a zraniteľnosť CVE-2026-70585 lokálny útočník s nízkymi oprávneniami.

Kritická zraniteľnosť sa nachádza aj v komponente **Microsoft Windows Media Foundation**. CVE-2026-69601 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.

Tri kritické zraniteľnosti sa nachádzajú v komponente **Windows Hyper-V**. Zraniteľnosti CVE-2026-69603 a CVE-2026-80083 umožňujú lokálnym útočníkom s nízkymi oprávneniami **vykonávať kód**. Prvá súvisí s pretečením vyrovnávacej pamäte na halde, druhá vyplýva z dereferencie nedôveryhodného ukazovateľa. Zraniteľnosť CVE-2026-72961 súvisí s pretečením vyrovnávacej pamäte na halde a lokálnym útočníkom s administratívnym prístupom ku zraniteľnému Hyper-V hostiteľovi umožňuje **eskalovať svoje oprávnenia** na úroveň VTL1.

Kritická zraniteľnosť CVE-2026-69649 sa nachádza v komponente **Windows Raw Image Extension**. Súvisí s pretečením vyrovnávacej pamäte na halde. Zraniteľnosť môže zneužiť neautorizovaný útočník na **vzdialené vykonanie kódu**. Potrebuje k tomu presvedčiť obeť, aby pristúpila ku zložke obsahujúcej špeciálne vytvorený súbor formátu RAW. Zraniteľnosť je možné zneužiť pri generovaní thumbnailu alebo náhľadu súboru.

Aj komponent **Microsoft WebP Image Extension** obsahuje podobnú zraniteľnosť, ktorá okrem pretečenia vyrovnávacej pamäte na halde súvisí aj s pretečením celočíselnej premennej. CVE-2026-70351 umožňuje útočníkom bez oprávnení **vzdialene vykonávať kód**.

Kritická zraniteľnosť CVE-2026-69676 komponentu **Windows Kerberos** umožňuje obísť autentifikáciu pomocou techniky capture-relay. Pre jej zneužitie potrebuje útočník s nízkymi oprávneniami poslať špeciálne vytvorenú požiadavku zraniteľnej služby, čo mu umožní

vzdialené vykonanie kódu. Na to potrebujú presvedčiť obeť, aby otvorila špeciálne vytvorený súbor.

Komponent **Windows Hello** obsahuje deväť kritických zraniteľností. Zraniteľnosť CVE-2026-72980 súvisí s nekontrolovaným prvkom vo vyhľadávacej ceste a lokálnym útočníkom s vysokými oprávneniami umožňuje **obchádzať bezpečnostné prvky**. Ostatné zraniteľnosti dovoľujú lokálnym útočníkom **eskalovať oprávnenia**. CVE-2026-69710 a CVE-2026-69799 vyplývajú zo vzniku súbehu procesov. CVE-2026-69725 súvisí s dvojitém uvoľnením pamäte. CVE-2026-69740, CVE-2026-69784 a CVE-2026-69864 súvisia s možnosťou použitia dealokovaného miesta v pamäti. CVE-2026-69820 a CVE-2026-81354 súvisia s pretečením vyrovnávacej pamäte na halde.

Kritická zraniteľnosť CVE-2026-69712 **Windows Key Distribution Center** je spôsobená možnosťou použitia dealokovaného miesta v pamäti. vzdialený útočník s nízkymi oprávneniami ju môže zneužiť na **vzdialené vykonanie kódu**.

Kritické zraniteľnosti komponentu **Windows DNS Server** dovoľujú neautorizovanému útočníkovi **vzdialené vykonanie kódu**. CVE-2026-69730, CVE-2026-69813, CVE-2026-69858, CVE-2026-72987 a CVE-2026-77505 súvisia s možnosťou použitia dealokovaného miesta v pamäti. CVE-2026-69827 súvisí okrem možnosti použitia dealokovaného miesta v pamäti tiež so vznikom súbehu procesov, ktorý musí útočník vyhrať pre úspešné zneužitie tejto zraniteľnosti.

Kritická zraniteľnosť sa nachádza v komponente **Windows HTTP Print Provider**. CVE-2026-69769 súvisí s pretečením vyrovnávacej pamäte na halde. Zraniteľnosť môže zneužiť neautorizovaný útočník na **vzdialené vykonanie kódu**.

Podobnú kritickú zraniteľnosť obsahuje tiež komponent **Windows Shell**. CVE-2026-69829 súvisí s pretečením vyrovnávacej pamäte na halde. Zraniteľnosť môže zneužiť neautorizovaný útočník na **vzdialené vykonanie kódu**.

Dve kritické zraniteľnosti komponentu **Windows DHCP Server** umožňujú neautorizovaným útočníkom **vzdialené vykonávanie kódu**. CVE-2026-69845 vyplýva z pretečenia vyrovnávacej pamäte na halde a nevhodnej validácie vstupov. CVE-2026-72979 umožňuje použiť dealokované miesto v pamäti.

Windows ALPC obsahuje kritickú zraniteľnosť CVE-2026-69874, ktorá dovoľuje lokálnemu útočníkovi s vysokými oprávneniami **eskalovať svoje oprávnenia**. Súvisí s neošetrovanou dereferenciou nedôveryhodných ukazovateľov.

Podobnú zraniteľnosť s označením CVE-2026-69892 obsahuje aj komponent **Windows Virtual Trusted Platform Module**. Zraniteľnosť dovoľuje použiť dealokované miesto v pamäti.

Komponent **Windows Media Player** obsahuje dve kritické zraniteľnosti súvisiace a pretečením vyrovnávacej pamäte na halde. CVE-2026-70203 a CVE-2026-72960 umožňujú útočníkom bez

oprávnení **vzdialene vykonávať kód**. Na to potrebujú presvedčiť obeť, aby otvorila špeciálne vytvorený mediálny súbor.

Komponent **Windows Paint** obsahuje kritickú zraniteľnosť súvisiacu s pretečením vyrovnávacej pamäte na halde. CVE-2026-70586 umožňuje útočníkom bez oprávnení **vzdialene vykonávať kód**. Na to potrebujú presvedčiť obeť, aby otvorila špeciálne vytvorený súbor.

Kritické zraniteľnosti CVE-2026-72954 a CVE-2026-72957 komponentu **Windows Deployment Services** umožňujú útočníkom s nízkymi oprávneniami **vykonanie kódu**. Prvá súvisí s možnosťou použitia dealokovaného miesta v pamäti a môže ju zneužiť vzdialený útočník. Druhá vyplýva z pretečenia vyrovnávacej pamäte na halde a zneužiť ju môže lokálny útočník.

Kritická zraniteľnosť v komponente **Windows Credential Guard** CVE-2026-72958 súvisí s dvojitém uvoľnením pamäte. Zraniteľnosť môže zneužiť lokálny útočník s vysokými oprávneniami na **eskaláciu svojich oprávnení** na úroveň VTL1. Potrebuje na to vyhrať súbeh procesov.

Kritická zraniteľnosť CVE-2026-72962 ovládača **Windows USB Video Driver** je spôsobená pretečením vyrovnávacej pamäte na halde. Lokálny útočník s vysokými oprávneniami ju môže zneužiť na **zvýšenie svojich oprávnení** na úroveň Virtual Trust Level 1 (VTL1).

Kritická zraniteľnosť CVE-2026-72981 komponentu **IP Helper**, zraniteľnosť CVE-2026-72983 komponentu **Internet Connection Sharing (ICS)** a zraniteľnosť CVE-2026-73009 komponentu **Windows Secure Socket Tunneling Protocol (SSTP)** umožňujú použiť dealokované miesto v pamäti. Pre ich zneužitie potrebuje neautentifikovaný útočník poslať špeciálne vytvorený paket zraniteľnej služby, čo mu umožní **vzdialené vykonanie kódu**.

Kritická zraniteľnosť CVE-2026-72982 komponentu **Windows Netlogon** je spôsobená pretečením vyrovnávacej pamäte na zásobníku. Pre jej zneužitie potrebuje neautentifikovaný útočník poslať špeciálne vytvorený paket zraniteľnej služby, čo mu umožní **vzdialené vykonanie kódu**.

Komponent **Graphic Fonts** obsahuje dve kritické zraniteľnosti súvisiace s pretečením vyrovnávacej pamäte na halde a pretečením celočíselnej premennej. CVE-2026-72986 a CVE-2026-73018 umožňujú útočníkom bez oprávnení **vzdialene vykonávať kód**. Na to potrebujú presvedčiť obeť, aby otvorila špeciálne vytvorený súbor.

V komponente **DirectWrite** sa nachádza kritická zraniteľnosť súvisiaca s pretečením vyrovnávacej pamäte na zásobníku. CVE-2026-73006 umožňuje útočníkom bez oprávnení **vzdialene vykonávať kód**. Na to potrebujú presvedčiť obeť, aby otvorila špeciálne vytvorený súbor.

V komponente **Microsoft Failover Cluster** boli opravené dve kritické chyby zabezpečenia. Zraniteľnosť CVE-2026-73010 umožňuje použiť dealokované miesto v pamäti a CVE-2026-78444 je spôsobená neošetrenou dereferenciou nedôveryhodného ukazovateľa. Pre ich

zneužitie potrebuje neautentifikovaný útočník poslať špeciálne vytvorený paket zraniteľnej služby, čo mu umožní **vzdialené vykonanie kódu**. Pre zneužitie druhej potrebuje tiež vyhrať súbeh procesov.

Komponent **Graphics Kernel** obsahuje kritickú zraniteľnosť CVE-2026-73017, ktorá súvisí s pretečením vyrovnávacej pamäte na halde. Lokálnym útočníkom s vysokými oprávneniami umožňuje **vykonávať kód**. Na to potrebujú poznať cieľový systém a mať možnosť nastaviť podmienky pre vytvorenie nešpecifikovanej podmienky. Podobná kritická zraniteľnosť CVE-2026-81355 bola opravená aj v ovládači **Virtual Hard Disk (VHD) Miniport**.

Dve kritické zraniteľnosti komponentu **Windows Graphics Component** umožňujú neautorizovaným útočníkom **vzdialené vykonávanie kódu**. CVE-2026-77493 súvisí s dvojitém uvoľnením pamäte a CVE-2026-81955 vyplýva z pretečenia vyrovnávacej pamäte na halde. Pre ich zneužitie potrebujú útočníci presvedčiť obeť, aby otvorila špeciálne vytvorený súbor RTF. Pre zneužitie prvej postačí vygenerovanie náhľadu škodlivého súboru (Preview Pane).

Kritická zraniteľnosť CVE-2026-81352 v knižnici **Microsoft Windows Codecs Library**, konkrétne vo **Web Media Extensions** je spôsobená pretečením vyrovnávacej pamäte na halde. Útočník bez oprávnení ju môže zneužiť na **vzdialené vykonanie kódu**.

Komponent **Windows Virtualization-Based Security (VBS)** obsahuje dve kritické zraniteľnosti. CVE-2026-83498 súvisí s neošetrenou dereferenciou nedôveryhodného ukazovateľa a umožňuje získať **zvýšené oprávnenia**. Zraniteľnosť CVE-2026-83501 vyplýva z možnosti čítania pamäte mimo povolené hodnoty a môže viesť k **úniku citlivých informácií**. Zraniteľnosti môže zneužiť lokálny útočník s nízkymi oprávneniami.

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

ZRANITEĽNÉ SYSTÉMY:

- HEIF Image Extension
- HEVC Video Extensions
- HEVC Video Extensions for Licensed Applications
- HEVC Video Extensions from Device Manufacturer
- Raw Image Extension
- Remote Desktop client for Windows Desktop
- SQL Server Management Studio 22
- Web Media Extensions
- WebP 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 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-2026-58599>

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65669>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69499>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69501>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69518>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69530>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69579>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69590>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69595>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69601>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69603>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69649>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69676>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69710>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69712>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69725>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69730>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69740>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69769>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69784>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69799>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69813>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69820>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69827>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69829>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69845>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69846>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69852>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69858>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69860>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69864>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69874>

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69890>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69906>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70203>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70296>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70351>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70585>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70586>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72950>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72954>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72957>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72958>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72959>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72960>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72961>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72962>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72979>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72980>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72981>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72982>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72983>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72986>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72987>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73006>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73009>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73010>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73013>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73017>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73018>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73023>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77493>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77495>

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77504>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77505>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78444>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78445>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78449>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78450>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-80083>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81352>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81354>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81355>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81955>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83498>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83501>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83939>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85921>

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

Spoločnosť Microsoft v roku 2025 plánuje ukončiť 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 plánuje ukončiť podporu pre v súčasnosti podporované verzie nasledovne:

23H2 Enterprise a Education: Podpora skončí 10. novembra 2026.

24H2 Home a Pro: Podpora skončí 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. 26H1.

2. KANCELÁRSKE BALÍKY MICROSOFT OFFICE A OFFICE WEB APPS

Spoločnosť Microsoft vydala v mesiaci september bezpečnostné aktualizácie, ktoré opravujú 28 kritických a 116 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Aplikácia **Skype for Business** obsahuje kritickú zraniteľnosť CVE-2026-66302, ktorá umožňuje neautentifikovanému útočníkovi **vzdialene vykonávať kód**. Súvisí s neošetrenou kontrolou nad súborovými cestami a názvami súborov. Pre jej zneužitie útočník nepotrebuje interakciu obeť. Stačí, keď pošle špeciálne vytvorenú požiadavku, ktorou zapíše svoj súbor na ľubovoľné miesto na zraniteľnom serveri.

Dve kritické zraniteľnosti bolo opravené v **Microsoft Office Graphics Component**. Neautorizovaný útočník ich môže zneužiť na **vzdialené vykonanie kódu**. Na to potrebuje poslať obeť škodlivý súbor a presvedčiť ju, aby ho otvorila. Zraniteľnosť CVE-2026-78439 spôsobuje pretečenie vyrovnávacej pamäte zásobníka. CVE-2026-81955 vyplýva z pretečenia vyrovnávacej pamäte na halde. Náhľad dokumentu (Preview Pane) pre ne nepredstavuje vektor útoku.

Balíky **Microsoft Office** obsahujú štyri kritické zraniteľnosti, ktoré umožňujú neautorizovaným útočníkom **vzdialené vykonávanie kódu**. Zraniteľnosti CVE-2026-69285, CVE-2026-77898 a CVE-2026-78505 sú spôsobené pretečením vyrovnávacej pamäte na halde. CVE-2026-69632 vyplýva z možnosti opätovného použitia dealokovaného miesta v pamäti. Ich zneužitie si spravidla vyžaduje, aby útočník presvedčil obeť, aby otvorila špeciálne pripravený súbor MS Office. Útočným vektorom aj náhľad dokumentu (Preview Pane).

Tri kritické zraniteľnosti boli opravené v **Microsoft Office PowerPoint**. Neautorizovaný útočník ich môže zneužiť na **vzdialené vykonávanie kódu**. CVE-2026-69678, CVE-2026-69767 a CVE-2026-69797 vyplývajú z možnosti opätovného použitia dealokovaného miesta v pamäti. Pre ich zneužitie musí útočník presvedčiť obeť, aby otvorila špeciálne pripravený súbor MS Office. Útočným vektorom môže byť aj náhľad dokumentu (Preview Pane).

V **Microsoft Outlook** boli opravené štyri kritické zraniteľnosti. Tri z nich dovoľujú neautorizovaným útočníkom **vzdialené vykonávanie kódu**. CVE-2026-78509 je spôsobená pretečením vyrovnávacej pamäte na halde. Jej zneužitie nevyžaduje interakciu obeť. CVE-2026-78519 a CVE-2026-78525 si vyžadujú interakciu obeť, no vektorom útoku môže byť aj vygenerovanie náhľadu škodlivého e-mailu (Preview Pane). Prvá vzniká kvôli možnosti použitia neinicializovaných zdrojov, druhá dovoľuje opätovne použiť dealokované miesto v pamäti. Štvrtá chyba zabezpečenia CVE-2026-78520 dovoľuje vzdialenému neautorizovanému útočníkovi získať **prístup k citlivým informáciám** umožnením čítania pamäte haldy mimo povolené hodnoty. Aj pre jej zneužitie postačuje vygenerovanie náhľadu škodlivého e-mailu (Preview Pane).

V aplikáciách **Microsoft Outlook** a **Word** bola opravená kritická zraniteľnosť CVE-2026-78510, ktorá súvisí s pretečením vyrovnávacej pamäte na halde. Neautorizovaný útočník ju môže zneužiť na **lokálne vykonanie ľubovoľného kódu**. Útočným vektorom môže byť aj náhľad dokumentu (Preview Pane).

V **Microsoft Word** bola opravená kritická zraniteľnosť, ktorú môže neautorizovaný útočník zneužiť na **vzdialené vykonávanie kódu**. CVE-2026-81952 je spôsobená pretečením vyrovnávacej pamäte na halde. Pre ich zneužitie musí útočník presvedčiť obeť, aby otvorila špeciálne pripravený súbor RTF. Náhľad dokumentu (Preview Pane) pre ňu nepredstavuje vektor útoku.

Šesť kritických zraniteľností bolo opravených aj v aplikácii **Microsoft Excel**. Neautorizovaný útočník ich môže zneužiť na **lokálne vykonanie ľubovoľného kódu**. CVE-2026-81948 a CVE-2026-81951 je spôsobená pretečením vyrovnávacej pamäte na halde. CVE-2026-81959 okrem pretečenia na halde súvisí a s pretečením celočíselnej premennej. Chybu zabezpečenia CVE-2026-81949 spôsobuje tiež pretečenie celočíselnej premennej. CVE-2026-81950 vyplýva z dvojitého uvoľnenia pamäte. Posledná zraniteľnosť CVE-2026-81953 vyplýva z pretečenia vyrovnávacej pamäte zásobníka. Pre zneužitie zraniteľností musí útočník presvedčiť obeť, aby otvorila špeciálne pripravený súbor MS Office. Náhľad dokumentu (Preview Pane) pre ne nepredstavuje vektor útoku.

Štyri kritické zraniteľnosti spojené s produktami **Microsoft 365 Copilot** opravila spoločnosť Microsoft na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre ich odstránenie. Zraniteľnosť CVE-2026-85885 umožňovala vzdialeným neautorizovaným útočníkom **eskalovať oprávnenia** kvôli nevhodne neutralizovaným špeciálnym prvkom používaným v príkazoch. Chybu zabezpečenia CVE-2026-85887 mohol na diaľku zneužiť útočník s nízkymi oprávneniami pre **získanie citlivých informácií** kvôli nesprávne pridelovaným oprávneniam. Zraniteľnosť s označením CVE-2026-78501 zasahovala službu **Business Chat** a neautorizovanému vzdialenému útočníkovi dovoľovala **získať prístup k citlivým informáciám**. Chyba zabezpečenia súvisela s nevhodnou neutralizáciou špeciálnych prvkov používaných v príkazoch. Posledná zraniteľnosť CVE-2026-80098 zasahovala produkt **Copilot Studio** a umožňovala vzdialeným neautorizovaným útočníkom **eskalovať oprávnenia**. Spôsobená bola nevhodným spôsobom verifikácie kryptografického podpisu.

otvoreným presmerovaním, resp. presmerovaním URL na nedôveryhodné zdroje. Zraniteľnosť CVE-2026-50517 súvisí s deserializáciou nedôveryhodných dát, čo umožňuje útočníkom s nízkymi oprávneniami **vzdialene vykonávať kód**.

Microsoft Fabric obsahuje dve kritické zraniteľnosti, ktoré umožňujú vzdialenému útočníkovi **navýšiť svoje oprávnenia**. CVE-2026-69843 umožňuje útočníkovi obísť autentifikáciu pomocou spoofingu. CVE-2026-70178 vyplýva z absentujúceho mechanizmu autorizácie a zneužiť ju môže útočník s nízkymi oprávneniami. Spoločnosť Microsoft chyby zabezpečenia opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre ich odstránenie.

Vysoko závažné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu, navýšenie privilégií, získavanie citlivých informácií, spôsobenie nedostupnosti systémov (DoS) a spoofingové útoky**.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft 365 Copilot
- Microsoft 365 Copilot's Business Chat
- Microsoft Access 2016 (32-bit edition)
- Microsoft Access 2016 (64-bit edition)
- Microsoft Authenticator for Android
- Microsoft Copilot Studio
- Microsoft Excel 2016 (32-bit edition)
- Microsoft Excel 2016 (64-bit edition)
- Microsoft Fabric
- 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 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 Outlook 2016 (32-bit edition)
- Microsoft Outlook 2016 (64-bit edition)
- Microsoft PowerPoint 2016 (32-bit edition)
- Microsoft PowerPoint 2016 (64-bit edition)
- Microsoft Publisher 2016 (32-bit edition)
- Microsoft Publisher 2016 (64-bit edition)
- Microsoft SharePoint Server Subscription Edition
- Microsoft Teams for Android
- Microsoft Word 2016 (32-bit edition)
- Microsoft Word 2016 (64-bit edition)
- Office Online Server
- 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.msrm.microsoft.com/en-us/security-guidance>
- <https://msrm.microsoft.com/update-guide/vulnerability/CVE-2026-66302>
- <https://msrm.microsoft.com/update-guide/vulnerability/CVE-2026-69285>
- <https://msrm.microsoft.com/update-guide/vulnerability/CVE-2026-69632>
- <https://msrm.microsoft.com/update-guide/vulnerability/CVE-2026-69678>
- <https://msrm.microsoft.com/update-guide/vulnerability/CVE-2026-69767>

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69797>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69843>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70178>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77898>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78439>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78501>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78505>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78509>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78510>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78519>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78520>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78525>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-80098>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81948>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81949>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81950>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81951>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81952>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81953>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81955>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81959>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85885>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85887>

Koniec podpory pre Office 2016, Office 2019 a Office 2021

Spoločnosť Microsoft v roku 2025 plánuje ukončiť podporu pre Office 2016 a Office 2019. Po dátume 14. decembra 2025 už tieto produkty nedostávajú aktualizácie zabezpečenia, aktualizácie nesúvisiace so zabezpečením, opravy chýb, technickú podporu a ani aktualizácie technického obsahu online.

Podpora pre balík [Microsoft Office 2021](#) bude ukončená 13. októbra 2026.

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 september opravila 4 vysoko závažné zraniteľnosti vo webovom prehliadači Microsoft Edge.

Vysoko závažná zraniteľnosť CVE-2026-69486 dovoľuje neautorizovanému útočníkovi **vzdialene vykonávať škodlivý kód**. Pre jej úspešné zneužitie potrebuje presvedčiť obeť, aby otvorila špeciálne vytvorený súbor. Zraniteľnosť spočíva v pretečení vyrovnávacej pamäte na halde.

Dve závažné zraniteľnosti vyplývajú z možnosti opätovného použitia dealokovanej pamäte. Neautorizovaný útočník ich môže zneužiť na vykonávanie **navýšenie svojich oprávnení**. Pre úspešné zneužitie CVE-2026-85893 potrebuje vzdialený útočník presvedčiť obeť, aby vykonala úkony na podvrhutej škodlivej webstránke, ktoré aktivujú funkciu automatického dopĺňania. Úspešným zneužitím CVE-2026-88097 môže lokálny útočník uniknúť zo sandboxu prehliadača,

Vysoko závažná zraniteľnosť CVE-2026-85892 spočíva vo vzniku súbehu procesov. Keď ho lokálny útočník s nízkymi oprávneniami vyhrá, môže **eskalovať svoje oprávnenia** a uniknúť zo sandboxu prehliadača. Pre úspešné zneužitie zraniteľnosti potrebuje útočník presvedčiť obeť, aby vykonala úkony na podvrhutej škodlivej webstránke, ktoré aktivujú funkciu automatického dopĺňania.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft Edge (Chromium-based) verzie staršie ako 153.0.4234.48

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-2026-69486>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85892>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85893>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-88097>

MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci september opravila 83 vysoko závažných zraniteľností v líniiach internetových prehliadačov Firefox a Firefox ESR.

Línia Firefox ESR obsahuje vysoko závažnú zraniteľnosť CVE-2026-75874 v komponente Remote Settings Client, ktorá umožňuje **únik zo sandboxu**. Ďalšia zraniteľnosť tohto komponentu má označenie CVE-2026-92038 a zasahuje línie Firefox aj Firefox ESR. Spoločnosť Mozilla ju označila ako obídenie mitigácie.

Firefox for Android obsahuje zraniteľnosť CVE-2026-84117, ktorá umožňuje **eskaláciu oprávnení**.

V komponente JavaScript: GC sa nachádza vysoko závažná zraniteľnosť CVE-2026-84118, ktorá dovoľuje opätovné použitie dealokovanej pamäte. Zasahuje línie Firefox a Firefox ESR.

V komponente JavaScript: WebAssembly sa nachádza päť vysoko závažných zraniteľností. CVE-2026-100765, CVE-2026-100769 a CVE-2026-100776 dovoľujú opätovné použitie dealokovanej pamäte. CVE-2026-100788 vyplýva z neplatnej dereferencie ukazovateľa. CVE-2026-100792 súvisí s chybnou kompiláciou v nástroji JIT. Zraniteľnosti zasahujú línie Firefox a Firefox ESR.

Línia Firefox obsahuje vysoko závažnú zraniteľnosť CVE-2026-100793, ktorá súvisí s chybnou kompiláciou v nástroji JIT. Zasahuje komponent JavaScript Engine.

Línie Firefox a Firefox ESR obsahujú tri vysoko závažné zraniteľnosti v komponente DOM: Navigation. CVE-2026-84119 a CVE-2026-92025 súvisia s možnosťou opätovného použitia dealokovanej pamäte. Zneužitie prvej z nich môže viesť ku **úniku zo sandboxu**. Rovnaký dôsledok môže mať zneužitie CVE-2026-100758.

Chyba zabezpečenia CVE-2026-84121 línií Firefox a Firefox ESR v komponente DOM: Security dovoľuje opätovne použiť dealokovanú pamäť a umožňuje **únik zo sandboxu**.

Komponent DOM: Core & HTML obsahuje desať vysoko závažných zraniteľností. Osem z nich, CVE-2026-84124, CVE-2026-84125, CVE-2026-92028, CVE-2026-100772, CVE-2026-100774, CVE-2026-100780, CVE-2026-100785 a CVE-2026-100791, umožňuje opätovné použitie dealokovanej pamäte. Posledné dve, CVE-2026-92018 a CVE-2026-100778, môžu viesť k **úniku zo sandboxu**. Chyby zabezpečenia sú prítomné v líniiach Firefox, aj Firefox ESR.

Línia Firefox ESR obsahuje vysoko závažnú zraniteľnosť CVE-2026-16365 v komponente DOM: Workers, ktorá umožňuje **eskaláciu oprávnení**.

Línie Firefox a Firefox ESR obsahujú vysoko závažnú zraniteľnosť CVE-2026-92017 v komponente DOM: Service Workers, ktorá umožňuje **eskaláciu oprávnení**.

Chyba zabezpečenia CVE-2026-92022 línii Firefox a Firefox ESR v komponente DOM: HTML Parser umožňuje opätovné použitie dealokovanej pamäte.

Línie Firefox a Firefox ESR obsahujú vysoko závažnú zraniteľnosť CVE-2026-92027 v komponente DOM: Streams, ktorá dovoľuje opätovné použitie dealokovanej pamäte a CVE-2026-100771 súvisiacu s nešpecifikovaným nedefinovaným správaním.

Línia Firefox obsahuje vysoko závažnú zraniteľnosť CVE-2026-92037 v komponente DOM: Animation, ktorá vzniká kvôli nesprávne stanoveným hraničným podmienkam.

Chyby zabezpečenia CVE-2026-100762 a CVE-2026-100770 sa nachádzajú v komponente DOM: Content Processes. Zasahujú línie Firefox aj Firefox ESR a umožňujú **uniknúť zo sandboxu** kvôli možnosti opätovného použitia dealokovanej pamäte.

Línie Firefox a Firefox ESR obsahujú tri zraniteľnosti v komponente Audio/Video. Chyby zabezpečenia CVE-2026-84120 a CVE-2026-84122 súvisia s možnosťou opätovného použitia dealokovanej pamäte. Zraniteľnosť CVE-2026-100783 súvisí s neinicializovanou pamäťou.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť v komponente Audio/Video: Web Codecs. Chyba zabezpečenia CVE-2026-92005 súvisí s možnosťou opätovného použitia dealokovanej pamäte.

Vysoko závažná zraniteľnosť CVE-2026-100756 komponentu Audio/Video: Playback v líniiach Firefox a Firefox ESR vzniká kvôli nesprávne stanoveným hraničným podmienkam.

Šesť chýb zabezpečenia sa nachádza v komponente Graphics. CVE-2026-92035, CVE-2026-100775 a CVE-2026-100786, ktoré obsahujú línie Firefox a Firefox ESR, umožňujú **uniknúť zo sandboxu** kvôli možnosti opätovného použitia dealokovanej pamäte a nesprávne stanoveným hraničným podmienkam. Štvrtá chyba zabezpečenia s označením CVE-2026-100782, obsiahnutá v oboch líniiach, umožňuje kvôli nesprávne stanoveným hraničným podmienkam **eskaláciu oprávnení**. Chyba v rámci izolácie stránok CVE-2026-92034 sa nachádza v línii Firefox. Poslednú zraniteľnosť s označením CVE-2026-92014 obsahuje línia Firefox ESR. Vyplyva z nesprávne stanovených hraničných podmienok a umožňuje **eskaláciu oprávnení**.

Línia Firefox obsahuje štyri zraniteľnosti v komponente Graphics: WebGPU. Chyby zabezpečenia CVE-2026-100761 a CVE-2026-100768 umožňujú opätovne použiť dealokovanú pamäť, pričom prvá môže viesť ku **eskalácii oprávnení** útočníka. Zraniteľnosti CVE-2026-100764 a CVE-2026-100763 vyplývajú z nesprávne stanovených hraničných podmienok a prvá z nich tiež umožňuje **eskaláciu oprávnení**. Chyba CVE-2026-84123 opravená v tomto komponente vyplývajúca z možnosti opätovne použiť dealokovanú pamäť a umožňujúca **eskaláciu oprávnení** sa nachádza v líniiach Firefox a Firefox ESR.

Línie Firefox a Firefox ESR obsahujú osem zraniteľností v komponente Graphics: CanvasWebGL. Chyby zabezpečenia CVE-2026-92006, CVE-2026-92007, CVE-2026-92008, CVE-2026-92009, CVE-2026-92010, CVE-2026-92011, CVE-2026-92012, CVE-2026-92013 vyplývajú z nesprávne stanovených hraničných podmienok a umožňujú **eskaláciu oprávnení**.

Línie Firefox a Firefox ESR obsahujú dve zraniteľnosti v komponente Graphics: WebRender. Chyby zabezpečenia CVE-2026-92020 vyplýva z nesprávne stanovených hraničných podmienok a umožňujú **eskaláciu oprávnení**. CVE-2026-100781 umožňuje kvôli nesprávne stanoveným hraničným podmienkam **uniknúť zo sandboxu**.

Zraniteľnosti CVE-2026-100777 a CVE-2026-100789 komponentu Graphics: Canvas2D v líniiach Firefox a Firefox ESR vyplývajú z možnosti opätovného použitia dealokovanej pamäte. Línia Firefox ESR obsahuje tretiu rovnakú zraniteľnosť CVE-2026-100832.

Línia Firefox obsahuje vysoko závažnú zraniteľnosť CVE-2026-84126 v komponente Layout: Grid, ktorá vyplýva z nesprávne stanovených hraničných podmienok.

Zraniteľnosť CVE-2026-100784 komponentu Layout: Text and Fonts sa nachádza v líniiach Firefox a Firefox ESR. Súvisí s možnosťou opätovného použitia dealokovanej pamäte.

Komponent WebExtensions obsahuje vysoko závažnú zraniteľnosť CVE-2026-92015, ktorá umožňuje **eskaláciu oprávnení**. Nachádza sa v líniiach Firefox a Firefox ESR.

Komponent Disability Access APIs obsahuje vysoko závažnú zraniteľnosť CVE-2026-92016, ktorá dovoľuje opätovné použitie dealokovanej pamäte. Nachádza sa v líniiach Firefox a Firefox ESR.

Línia Firefox ESR obsahuje vysoko závažnú zraniteľnosť CVE-2026-92021 v komponente JavaScript Engine: JIT, ktorá dovoľuje opätovné použitie dealokovanej pamäte.

Línie Firefox a Firefox ESR obsahujú vysoko závažnú zraniteľnosť CVE-2026-92023 v komponente XML, ktorá dovoľuje opätovné použitie dealokovanej pamäte.

Línie Firefox a Firefox ESR obsahujú vysoko závažné zraniteľnosti CVE-2026-92024 a CVE-2026-92029 v komponente SVG, ktoré dovoľujú opätovné použitie dealokovanej pamäte.

Línie Firefox a Firefox ESR obsahujú vysoko závažnú zraniteľnosť CVE-2026-92026 v komponente Networking, ktorá dovoľuje opätovné použitie dealokovanej pamäte.

Zraniteľnosť CVE-2026-92036 komponentu Networking: HTTP sa nachádza v línii Firefox. Súvisí s nesprávne nastavenými hraničnými podmienkami.

Zraniteľnosť CVE-2026-100766 komponentu Networking: JAR sa nachádza v líniiach Firefox a Firefox ESR. Umožňuje **získavať citlivé informácie**.

Zraniteľnosť CVE-2026-100767 komponentu Networking: Cache v líniiach Firefox a Firefox ESR vyplýva z možnosti opätovného použitia dealokovanej pamäte.

Línie Firefox a Firefox ESR obsahujú vysoko závažnú zraniteľnosť CVE-2026-100757 v komponente Widget, ktorá dovoľuje opätovné použitie dealokovanej pamäte.

Vysoko závažná zraniteľnosť CVE-2026-100759 súvisí s neinicializovanou pamäťou. Nachádza sa v komponente Storage: Quota Manager a zasahuje línie Firefox aj Firefox ESR.

Chyba zabezpečenia CVE-2026-100773 línii Firefox a Firefox ESR v komponente Storage: IndexedDB umožňuje opätovné použitie dealokovanej pamäte.

Línie Firefox a Firefox ESR obsahujú vysoko závažnú zraniteľnosť CVE-2026-100760 v komponente Security: Process Sandboxing, ktorá umožňuje **únik zo sandboxu**.

Chyby zabezpečenia CVE-2026-100779 a CVE-2026-100790 línii Firefox a Firefox ESR v komponente XSLT umožňuje opätovné použitie dealokovanej pamäte.

Chyba zabezpečenia CVE-2026-100787 umožňuje **uniknúť zo sandboxu**. Zasahuje komponent XUL línii Firefox a Firefox ESR.

Identifikátory CVE-2026-84143, CVE-2026-84144 a CVE-2026-84145 v líniiach Firefox a Firefox ESR opisujú interne objavené sady chýb pri narábaní s pamäťou a iné bezpečnostné chyby, ktoré by podľa spoločnosti Mozilla mohli byť zneužíteľné.

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox verzie staršej ako 157
- Mozilla Firefox ESR verzie staršej ako 115.42, 140.17 a 153.4

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 157 a Firefox ESR na verziu 115.42, 140.17 alebo 153.4.

ZDROJE:

- <https://www.mozilla.org/en-US/security/advisories/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-82/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-83/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-84/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-85/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-90/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-91/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-92/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-93/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-97/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-98/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-99/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-100/>

GOOGLE CHROME

V mesiaci september spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 22 kritických a 138 vysoko závažných zraniteľností.

Komponent **AdFilter** obsahuje kritickú zraniteľnosť CVE-2026-95310, ktorá umožňuje opätovné použitie dealokovanej pamäte.

Komponent **ANGLE** obsahuje štyri kritické zraniteľnosti, ktoré vyplývajú z pretečenia nešpecifikovanej vyrovnávacej pamäte. Chyby zabezpečenia dostali identifikátory CVE-2026-95281, CVE-2026-95284, CVE-2026-95350 a CVE-2026-102331.

Komponent **Cast** obsahuje kritickú zraniteľnosť CVE-2026-87628, ktorá umožňuje opätovné použitie dealokovanej pamäte.

Chybu zabezpečenia umožňujúcu opätovné použitie dealokovanej pamäte obsahuje tiež komponent **Fullscreen**. Dostala označenie CVE-2026-95313.

Dve kritické chyby zabezpečenia v komponente **GPU** umožňujú zápis do pamäte mimo povolené hodnoty. Dostali identifikátory CVE-2026-95322 a CVE-2026-95357.

Komponent **Internals** obsahuje kritickú zraniteľnosť CVE-2026-91721, ktorá umožňuje opätovné použitie dealokovanej pamäte.

Chybu zabezpečenia umožňujúcu opätovné použitie dealokovanej pamäte obsahuje tiež komponent **ServiceWorker**. Dostala označenie CVE-2026-95339.

Opätovné použitie dealokovanej pamäte umožňuje aj kritická zraniteľnosť CVE-2026-84353 komponentu **Shared Tab Groups**.

Osem kritických zraniteľností bolo opravených v komponente **WebGL**. Chyby zabezpečenia CVE-2026-84352, CVE-2026-87464 a CVE-2026-87488 umožňujú opätovné použitie dealokovaného miesta v pamäti. CVE-2026-87438 a CVE-2026-95329 dovoľujú zápis do pamäte mimo povolené hodnoty a CVE-2026-91726 dovoľuje čítanie pamäte. CVE-2026-87527 a CVE-2026-95349 súvisia s pretečením nešpecifikovanej vyrovnávacej pamäte.

Kritická chyba zabezpečenia v komponente **WindowDialog** umožňuje opätovné použitie dealokovanej pamäte. Dostala identifikátor CVE-2026-95356.

Komponent **Workers** obsahuje kritickú zraniteľnosť CVE-2026-91749, ktorá umožňuje opätovné použitie dealokovanej pamäte.

Spoločnosť Google opravila vysoko závažné zraniteľnosti v komponentoch **Android**, **ANGLE**, **Aura**, **Auth**, **Bindings**, **Bluetooth**, **Browser**, **CacheStorage**, **Codecs**, **Composing**, **Core**, **CrashReporting**, **DataTransfer**, **Dawn**, **Device**, **DevTools**, **DigitalCredentials**, **DOM**, **Extensions**, **FileSystem**, **FullScreen**, **GPU**, **HID**, **Chromecast**, **Chromoting**, **IndexedDB**, **Input**, **Media**, **Mobile**, **Mojo**, **Navigation**, **Network**, **Omnibox**, **Paint**, **Passwords**, **Payments**, **PDF**, **PDFium**, **PictureInPicture**, **Platform**, **PlatformIntegration**, **Printing**, **Proxy**, **Receiver**, **SecurityIndicators**, **ServiceWorker**, **Skia**, **Tint**, **TrustedWebActivities**, **Updater**, **V8**, **Video**, **Views**, **WebAppInstalls**, **WebAudio**, **WebAuthentication**, **WebGL**, **WebGPU**, **WebPackaging**, **WebUI**. Tieto dovoľujú čítať a zapisovať do pamäte mimo povolené hodnoty, použiť dealokovanú pamäť a neinicializované zdroje, súvisia s pretečením medzipamäte zásobníka či celočíselnej premennej, vyplývajú zo zámeny typu premennej, dvojitého uvoľnenia pamäte, vzniku súbehu procesov, nedostatočnej validácie nedôveryhodných vstupov. Súvisia s chybami pamäte, autorizácie a zobrazenia, rozpoznávania referencií a nedostatočnej kontrole zdrojov. Umožňujú získavať citlivé informácie a vykonávať XSS.

Vývojári spoločnosti Google opravili tiež **aktívne zneužívanú** vysoko závažnú zraniteľnosť [CVE-2026-87491](#) v komponente **V8**, ktorá umožňuje **vzdialene vykonávať kód v rámci sandboxu**. Zraniteľnosť súvisí s možnosťou zápisu do pamäte mimo povolené hodnoty.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows verzie staršej ako 154.0.8037.92/.93
- Google Chrome pre Mac verzie staršej ako 154.0.8037.92/.93

- Google Chrome pre Linux verzie staršej ako 154.0.8037.92

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows aspoň na verziu 154.0.8037.92/.93, Mac aspoň na verziu 154.0.8037.92/.93 a Linux aspoň na verziu 154.0.8037.92.

ZDROJE:

- <https://chromereleases.googleblog.com/2026/09>
- <https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop.html>
- https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html
- https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html
- https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html
- https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0856730748.html
- https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_01807488085.html

4. ADOBE ACROBAT A READER

V mesiaci september spoločnosť Adobe opravila 20 vysoko závažných zraniteľností v produktoch Adobe Acrobat a Reader.

Vysoko závažná zraniteľnosť CVE-2026-81996 súvisí s nesprávne fungujúcim mechanizmom autorizácie. Lokálny útočník s nízkymi oprávneniami ju môže zneužiť na **eskaláciu svojich oprávnení**.

Ďalšia opravená vysoko závažná zraniteľnosť vzniká kvôli nevhodne implementovanej kontrole modifikácie atribútov prototypu objektu (Prototype Pollution). CVE-2026-81994 môže lokálny útočník bez autorizácie zneužiť na **čítanie ľubovoľných súborov s súborovom systému**.

Zraniteľnosti CVE-2026-81983, CVE-2026-79908, CVE-2026-81979, CVE-2026-81980 a CVE-2026-81981 súvisia s možnosťou zápisu do pamäte mimo povolené hodnoty. Lokálny útočník bez autorizácie ich môže zneužiť na **vykonanie ľubovoľného kódu**.

Väčšina opravených zraniteľností vyplýva z možnosti opätovného použitia dealokovaného miesta v pamäti. Chyby zabezpečenia CVE-2026-79909, CVE-2026-81973, CVE-2026-81975, CVE-2026-81976, CVE-2026-81985, CVE-2026-81986, CVE-2026-81988, CVE-2026-81989 a CVE-2026-81990 môže lokálny útočník bez autorizácie zneužiť na **vykonanie ľubovoľného kódu**.

Vysoko závažná zraniteľnosť CVE-2026-79907 súvisí s dvojitém uvoľnením pamäte. Lokálny útočník bez autorizácie ju môže zneužiť na **vykonanie ľubovoľného kódu**.

Vysoko závažná zraniteľnosť CVE-2026-80161 vyplýva zo zámeny typu premennej. Lokálny útočník bez autorizácie ju môže zneužiť na **vykonanie ľubovoľného kódu**.

Vysoko závažná zraniteľnosť CVE-2026-81992 súvisí s pretečením vyrovnávacej pamäte haldy. Lokálny útočník bez autorizácie ju môže zneužiť na **vykonanie ľubovoľného kódu**.

Posledná opravená vysoko závažná zraniteľnosť vzniká kvôli pretečeniu celočíselnej premennej. CVE-2026-81987 môže lokálny útočník bez autorizácie zneužiť na **vykonanie ľubovoľného kódu**.

ZRANITEĽNÉ SYSTÉMY:

- Acrobat a Acrobat Reader pre Windows a Mac verzie 26.002.21900 a staršie
- Acrobat 2024 pre Windows a Mac verzie 24.001.30383 a staršie

ODPORÚČANIA:

Odporúčame aktualizáciu aspoň na verziu:

- Acrobat a Acrobat Reader pre Windows a Mac 26.002.21901
- Acrobat 2024 pre Windows a Mac 24.001.30429

ZDROJE:

- <https://helpx.adobe.com/security/security-bulletin.html#acrobat>
- <https://www.adobe.com/trust/security/products/acrobat/apsb26-141.html>

5. FRAMEWORKY

MICROSOFT .NET FRAMEWORK

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

Vysoko závažné zraniteľnosti spočívajú v nedostatočnej kontrole a ochrane vstupov a dát a v nesprávnej implementácii kontroly pôvodu dát/komunikácie. Súvisia s pretečením vyrovnávacej pamäte na halde a nevhodným narábaním s vysoko komprimovanými dátami. Väčšinu z nich môže zneužiť vzdialený útočník bez oprávnení. Umožňujú mu **navýšiť svoje oprávnenia, vzdialene vykonávať kód, získať prístup k citlivým informáciám a spôsobiť nedostupnosť služby (DoS)**.

ZRANITEĽNÉ SYSTÉMY:

- .NET 10.0 installed on Linux
- .NET 10.0 installed on Mac OS
- .NET 10.0 installed on Windows
- .NET 11.0 installed on Linux
- .NET 11.0 installed on Mac OS
- .NET 11.0 installed on Windows
- .NET 8.0 installed on Linux
- .NET 8.0 installed on Mac OS
- .NET 8.0 installed on Windows
- .NET 9.0 installed on Linux
- .NET 9.0 installed on Mac OS
- .NET 9.0 installed on Windows
- ASP.NET Core 10.0
- ASP.NET Core 11.0
- ASP.NET Core 8.0
- ASP.NET Core 9.0
- 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>

ORACLE JAVA

Spoločnosť Oracle plánuje vydať veľkú sadu opráv 20. október 2026.

ZDROJE:

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

INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

PRE ZÁVAŽNÚ ZRANITEĽNOSŤ V MICROSOFT EXCHANGE SERVER BOL ZVEREJNENÝ POC EXPLOIT

Spoločnosť Microsoft opravila v rámci augustových bezpečnostných aktualizácií vysoko závažnú zraniteľnosť v produkte Microsoft Exchange Server. Chyba zabezpečenia spočíva v možnosti obídenia autentifikácie metódou capture-replay. V kombinácii s ďalšími zraniteľnosťami umožňuje vzdialenému neautentifikovanému útočníkovi vykonanie ľubovoľného kódu s oprávneniami SYSTEM a získanie prístupu ku všetkým poštovým schránkam na serveri. Pre zraniteľnosť bol zverejnený proof-of-concept exploit. **Viac informácií na [stránke](#).**

KRITICKÁ ZRANITEĽNOSŤ APACHE TOMCAT

Vývojári Apache Tomcat opravili kritickú zraniteľnosť súvisiacu s nevhodným mechanizmom kontroly prístupov a pridelovania oprávnení. Chyba zabezpečenia umožňuje neautorizovanému vzdialenému útočníkovi obísť bezpečnostné obmedzenia. **Viac informácií na [stránke](#).**

V PAPER CUT MF A NG OPRAVILI DVE ZERO-DAY ZRANITEĽNOSTI

Spoločnosť PaperCut opravila dve aktívne zneužívané zero-day zraniteľnosti v serveroch PaperCut MF a NG. Jedna umožňuje obísť autentifikáciu a vykonať konfiguračné zmeny, druhá dovoľuje načítať a vykonať ľubovoľný kód v Java. Ich zreteľným ziskom neautentifikovaný útočník možnosť vzdialene vykonávať kód. Zatiaľ boli pozorované útoky smerujúce ku krádeži obsahu databázy. **Viac informácií na [stránke](#).**

AKTUALIZÁCIA KRITICKEJ ZRANITEĽNOSTI MIKROTIK ROUTEROS

Spoločnosť MikroTik zverejnila bezpečnostné aktualizácie operačného systému RouterOS vo všetkých podporovaných vetvách. Výrobca označuje aktualizáciu za dôležitú a odporúča jej bezodkladné nasadenie. **Viac informácií na [stránke](#).**

KRITICKÁ ZRANITEĽNOSŤ V ZARIADENIACH CISCO S TECHNOLOGIOU SILICON ONE

Spoločnosť Cisco zverejnila bezpečnostné upozornenie k zraniteľnosti CVE-2026-20212 v integrácii ASIC čipu Silicon One v prepínačoch Nexus 9000 Series. Vzdialený neautentifikovaný útočník môže zaslať špeciálne vytvorený vstup, ktorý je následne vykonaný ako kód s oprávneniami používateľa root. **Viac informácií na [stránke](#).**

KRITICKÁ ZRANITEĽNOSŤ RED HAT 389 DIRECTORY SERVER

Vývojári spoločnosti Red Hat opravili kritickú autentifikačnú chybu v komponente 389 Directory Server, ktorá umožňuje neautentifikovanému vzdialenému útočníkovi získať prístup na server s oprávneniami Directory Manager. **Viac informácií na [stránke](#).**

ZRANITEĽNOSTI VMWARE WORKSTATION A FUSION UMOŽŇUJÚ VYKONÁVAŤ KÓD

Spoločnosť Broadcom opravila v produktoch VMware Workstation a Fusion dve závažné zraniteľnosti umožňujúce útočníkovi s oprávneniami lokálneho administrátora na virtuálnom stroji vykonávať kód na hostiteľskom systéme. **Viac informácií na [stránke](#).**

GITLAB MÁ AKTÍVNE ZNEUŽÍVANÚ KRITICKÚ ZRANITEĽNOSŤ

Vývojári platformy GitLab opravili v rozhraní API aktívne neužívanú kritickú zraniteľnosť, ktorá umožňuje vzdialenému neautentifikovanému útočníkovi čítať ľubovoľné súbory na serveri GitLab. Okrem toho opravili jednu kritickú, šesť vysoko závažných a niekoľko ďalších zraniteľností. **Viac informácií na [stránke](#).**

AKTÍVNE ZNEUŽÍVANÁ KRITICKÁ ZRANITEĽNOSŤ CISCO ISE A ISE-PIC

Spoločnosť Cisco opravila aktívne zneužívanú kritickú zraniteľnosť v produktoch Cisco Identity Services Engine (ISE) a Cisco ISE Passive Identity Connector (ISE-PIC). Vzdialeným neautentifikovaným útočníkom umožňuje obísť autentifikáciu a získať prístup ku zraniteľnému zariadeniu. Okrem nej Cisco opravila ďalších 41 kritických zraniteľností v spomenutých produktoch. **Viac informácií na [stránke](#).**