MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

AUGUST 2026

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci august 20 kritických a 212 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritická zraniteľnosť CVE-2026-62815 v knižnici **Microsoft QUIC** súvisí s možnosťou použitia dealokovaného miesta v pamäti. Neautorizovaný útočník ju môže zneužiť na **vzdialené vykonanie kódu** zaslaním špeciálne vytvoreného paketu zraniteľnej službe.

Kritická zraniteľnosť CVE-2026-62816 v ovládači **Windows Reliable Multicast Transport Driver (RMCAST)** vyplýva z pretečenia vyrovnávacej pamäte na halde a pretečenia celočíselnej premennej. Neautorizovaný útočník ju môže zneužiť na **vzdialené vykonanie kódu** zaslaním špeciálne vytvoreného paketu zraniteľnej službe.

Kritické zraniteľnosti komponentu **Windows DNS Server** dovoľujú neautorizovanému útočníkovi **vzdialené vykonanie kódu**. CVE-2026-62817 umožňuje zapisovanie do pamäte mimo povolené hodnoty a dovoľuje útočníkovi posielať volania na ľubovoľné koncové body. CVE-2026-62820 súvisí so vznikom súbehu procesov. Neautentifikovaný útočník ju môže zneužiť poslaním špeciálne vytvoreného paketu zraniteľnej službe. CVE-2026-62878 vyplýva z pretečenia vyrovnávacej pamäte zásobníka, čo môže neautentifikovaný útočník dosiahnuť zaslaním špeciálne vytvoreného paketu zraniteľnej službe. Zraniteľnosť CVE-2026-65789 súvisí s možnosťou použitia dealokovaného miesta v pamäti. Zneužiť ju možno bez autentifikácie zaslaním špeciálne vytvoreného paketu zraniteľnej službe. Úspešné zneužitie môže vyžadovať splnenie určitých nešpecifikovaných technických požiadaviek.

Kritická zraniteľnosť CVE-2026-62818 sa nachádza vo **Windows Active Directory Certificate Services**. Súvisí s možnosťou použitia dealokovaného miesta v pamäti. Útočník s nízkymi oprávneniami ju môže zneužiť na **vzdialené vykonanie kódu**. Postačí mu na to zaslať špeciálne vytvorený paket zraniteľnej službe.

Kritická zraniteľnosť CVE-2026-62819 v komponente **Windows Routing and Remote Access Service (RRAS)** súvisí s možnosťou použitia dealokovaného miesta v pamäti. Útočník bez oprávnení ju môže zneužiť na **vzdialené vykonanie kódu**. Na to potrebuje zaslať špeciálne vytvorený paket zraniteľnej službe a vyhrať súbeh procesov.

Komponent **Windows GDI+** obsahuje dve kritické zraniteľnosti. CVE-2026-62822 súvisí s pretečením celočíselnej premennej a pretečením vyrovnávacej pamäte na halde. Umožňuje útočníkom bez oprávnení **vzdialene vykonávať kód.** Na to potrebujú presvedčiť obeť, aby otvorila špeciálne vytvorený súbor. Zraniteľnosť CVE-2026-62890 súvisí s pretečením vyrovnávacej pamäte na halde a dovoľuje lokálnemu útočníkovi s nízkymi oprávneniami **eskalovať svoje oprávnenia** až na úroveň SYSTEM.

Kritická zraniteľnosť CVE-2026-62823 komponentu **Windows DHCP Server** vyplýva z pretečenia vyrovnávacej pamäte na halde. Neautorizovaný útočník na priľahlej sieti ju môže zneužiť na **vzdialené vykonanie kódu**. Zneužiť ju možno poslaním špeciálne vytvoreného paketu zraniteľnej službe.

Kritická zraniteľnosť sa nachádza aj v komponente **Windows Remote Desktop Client**. CVE-2026-62824 súvisí s pretečením vyrovnávacej pamäte zásobníka. Zraniteľnosť môže zneužiť neautorizovaný útočník na **vzdialené vykonanie kódu**. Môže k tomu presvedčiť obeť, aby sa pripojila na jeho škodlivý server. Pri spracovaní odpovede servera môže vykonať kód na zraniteľnom klientovi.

Kritická zraniteľnosť v komponente **Windows Secure Socket Tunneling Protocol (SSTP)** CVE-2026-62889 súvisí s dvojitým uvoľnením pamäte. Zraniteľnosť môže zneužiť neautorizovaný útočník na **vzdialené vykonanie kódu**. Potrebuje na to poslať špeciálne vytvorený paket zraniteľnej službe a vyhrať súbeh procesov.

Kritická zraniteľnosť CVE-2026-62893 komponentu **Windows Deployment Services TFTP Server** umožňuje použiť dealokované miesto v pamäti. Pre jej zneužitie potrebuje útočník poslať špeciálne vytvorený paket zraniteľnej službe, čo mu umožní **vzdialené vykonanie kódu**.

Tri kritické zraniteľnosti sa nachádzajú v komponente **Windows iSCSI Target Service**. Zraniteľnosti CVE-2026-65679, CVE-2026-65791 a CVE-2026-65796 vyplývajú z pretečenia vyrovnávacej pamäte na halde a neautorizovaný útočník ich môže zneužiť na **vzdialené vykonávanie kódu**. Pre ich úspešné zneužitie potrebuje útočník poslať špeciálne vytvorený paket zraniteľnej službe.

Kritická zraniteľnosť CVE-2026-66799 **Windows Key Guard** je spôsobená pretečením vyrovnávacej pamäte na halde. Vzdialený útočník s nízkymi oprávneniami ju môže zneužiť na **zvýšenie svojich oprávnení** na úroveň Virtual Trust Level 1 (VTL1).

Kritická zraniteľnosť CVE-2026-66802 komponentu **Windows Device Health Attestation (DHA)** umožňuje použiť dealokované miesto v pamäti. Neautorizovaný útočník ju môže zneužiť na **vzdialené vykonanie kódu**. Zneužiť ju možno poslaním špeciálne vytvoreného paketu zraniteľnej službe, pričom útočník musí vyhrať súbeh procesov. Druhá kritická zraniteľnosť CVE-2026-71331 tohto komponentu súvisí s pretečením vyrovnávacej pamäte na halde a pretečením celočíselnej premennej. Pre jej zneužitie môže útočník poslať špeciálne vytvorený paket zraniteľnej službe.

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:

- 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 App for Mac
- Windows Remote Help
- 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-2026-62815
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62816
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62817
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62818
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62819
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62820
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62822
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62823
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62824
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62878
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62889
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62890
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62893
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65679
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65789
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65791
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65796
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-66799
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-66802
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-71331

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 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 august bezpečnostné aktualizácie, ktoré opravujú 30 kritických a 101 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Päť kritických zraniteľností bolo opravených v **Microsoft Office Graphics Component**. Neautorizovaný útočník ich môže zneužiť na **lokálne vykonanie ľubovoľného kódu**. Na to potrebuje poslať obeti škodlivý súbor MS Office a presvedčiť ju, aby ho otvorila. Zraniteľnosti CVE-2026-63513, CVE-2026-63519 a CVE-2026-65664 sú spôsobené pretečením vyrovnávacej pamäte na halde. CVE-2026-63526 a CVE-2026-66807 súvisia s pretečením vyrovnávacej

pamäte zásobníka. Útočným vektorom pre zneužitie zraniteľností môže byť aj náhľad dokumentu (Preview Pane), okrem zraniteľnosti CVE-2026-65664.

Balíky **Microsoft Office** obsahujú osem kritických zraniteľností, ktoré umožňujú neautorizovaným útočníkom **lokálne vykonávanie ľubovoľného kódu**. Pre šesť z nich je útočným vektorom aj náhľad dokumentu (Preview Pane). CVE-2026-63515 súvisí s pretečením celočíselnej premennej a možnosťou čítania pamäte mimo povolené hodnoty. CVE-2026-63532, CVE-2026-64898 a CVE-2026-64903 sú spôsobené pretečením vyrovnávacej pamäte na halde a celočíselnej premennej. CVE-2026-64909 spôsobuje pretečenie vyrovnávacej pamäte na halde a celočíselnej premennej a možnosť čítať pamäť mimo povolené hodnoty. CVE-2026-65657 vyplýva z možnosti opätovného použitia dealokovaného miesta v pamäti. Posledné dve nie je možné zneužiť pomocou Preview Pane. Chyba zabezpečenia CVE-2026-64910 vzniká kvôli neošetrenej dereferencii nedôveryhodných vstupov a zraniteľnosť CVE-2026-64911 súvisí s pretečením vyrovnávacej pamäte na halde a celočíselnej premennej. Pre zneužitie zraniteľností musí útočník presvedčiť obeť, aby otvorila špeciálne pripravený súbor MS Office.

Kritická zraniteľnosť CVE-2026-70130 balíkov **Microsoft Office** umožňuje neautorizovanému útočníkovi **lokálne vykonávať ľubovoľný kód**. Súvisí s pretečením vyrovnávacej pamäte na halde. Pre jej zneužitie útočník nepotrebuje interakciu obete.

V **Microsoft Word** boli opravené tri kritické zraniteľnosti, ktoré môže neautorizovaný útočník zneužiť na **lokálne vykonanie ľubovoľného kódu**. CVE-2026-63518 je spôsobená pretečením vyrovnávacej pamäte na halde, CVE-2026-63525 súvisí s chybou pri orezaní číselnej premennej a CVE-2026-64907 vyplýva z pretečenia vyrovnávacej pamäte zásobníka. Pre ich zneužitie musí útočník presvedčiť obeť, aby otvorila špeciálne pripravený súbor MS Office.

Tri kritické zraniteľnosti boli opravené aj v **Microsoft Excel**. Neautorizovaný útočník ich môže zneužiť na **lokálne vykonanie ľubovoľného kódu**. CVE-2026-68794 je spôsobená pretečením vyrovnávacej pamäte na halde, CVE-2026-68804 súvisí s pretečením vyrovnávacej pamäte na halde a chybou pri orezávaní číselnej premennej a CVE-2026-68816 vyplýva z pretečenia vyrovnávacej pamäte zásobníka. Pre ich zneužitie musí útočník presvedčiť obeť, aby otvorila špeciálne pripravený súbor MS Office. Náhľad dokumentu (Preview Pane) pre ne nepredstavuje vektor útoku.

Microsoft SharePoint Server obsahuje tri kritické zraniteľnosti. Zraniteľnosti s označením CVE-2026-62827 a CVE-2026-64921 súvisia s nevhodnou alebo absentujúcou autentifikáciou. Vzdialený útočník s nízkymi oprávneniami ich môže zneužiť pre **navýšenie svojich oprávnení**. Chyba zabezpečenia CVE-2026-65665 vyplýva z neošetrenej deserializácie nedôveryhodných dát. Vzdialený útočník s nízkymi oprávneniami ju môže zneužiť na **vzdialené vykonanie kódu**.

Kritická zraniteľnosť **Microsoft Office SharePoint** s označením CVE-2026-70332 súvisí s nevhodnou neutralizáciou vstupu. Vzdialený neautorizovaný útočník ju môže zneužiť pri

útokoch typu XSS, resp. **spoofingových útokoch**. Chybu zabezpečenia opravila spoločnosť Microsoft na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre jej odstránenie.

Kritickú zraniteľnosť CVE-2026-50515 v produkte **Azure Service Bus** a CVE-2026-62836 v produkte **Azure SQL Managed Instance** opravila spoločnosť Microsoft na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre ich odstránenie. Prvú zraniteľnosť, ktorá vyplýva z neošetrenej deserializácie nedôveryhodných dát, môže neautorizovaný vzdialený útočník zneužiť na **vzdialené vykonanie kódu**. Druhá zraniteľnosť súvisí s nevhodným obmedzením komunikácie na koncové body a neautorizovanému vzdialenému útočníkovi dovoľuje **navýšenie svojich oprávnení**.

Tri kritické zraniteľnosti v **Microsoft Teams** opravila spoločnosť Microsoft na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre ich odstránenie. Dve zraniteľnosti dovoľujú vzdialeným útočníkom **navýšiť svoje oprávnenia**. CVE-2026-62896, ktorá vyplýva z nevhodne nastaveného mechanizmu autentifikácie, môže zneužiť útočník s nízkymi oprávneniami. CVE-2026-65667 súvisí s chýbajúcou autorizáciou a pre zneužitie nevyžaduje žiadne oprávnenia. Chyba zabezpečenia CVE-2026-62918 súvisí s nevhodným spôsobom verifikácie kryptografického podpisu. Vzdialeným neautorizovaným útočníkom umožňuje vykonávať **spoofingové útoky**.

Microsoft Fabric obsahuje kritickú zraniteľnosť CVE-2026-63509, ktorá umožňuje prechádzanie relatívnymi cestami. Vzdialený útočník s nízkymi oprávneniami ich môže zneužiť pre **navýšenie svojich oprávnení**. Spoločnosť Microsoft chybu 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**, **zásahy do systémov** a **spoofingové útoky**.

ZRANITEĽNÉ SYSTÉMY:

- App Installer
- Azure Service Bus
- Azure SQL Managed Instance
- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft Access 2016 (32-bit edition)
- Microsoft Access 2016 (64-bit edition)
- 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 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 SharePoint Enterprise Server 2016
- Microsoft SharePoint Online
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription Edition
- Microsoft Teams
- Microsoft Teams for Android
- Microsoft Teams for iOS
- Microsoft Word 2016 (32-bit edition)
- Microsoft Word 2016 (64-bit edition)
- Office Online Server
- OneDrive for MacOS

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-2026-50515
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62827
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62836
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62896
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62918
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-63509
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-63513
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-63515
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-63518
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-63519
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-63525
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-63526
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-63532
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-64898
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-64903
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-64907
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-64909
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-64910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-64911
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-64921
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65657
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65664
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65665

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65667
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-66807
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68794
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68804
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68816
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70130
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70332

Koniec podpory pre Office 2016, Office 2019 a Office 2021

Spoločnosť Microsoft v roku 2025 plánovane ukončila 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 2021 alebo Office 2024), cloudovú verziu Office 365 alebo používať Office LTSC. Viac informácií na stránke výrobcu.

3. INTERNETOVÉ PREHLIADAČE

MICROSOFT EDGE

Spoločnosť Microsoft v mesiaci august opravila 6 vysoko závažných zraniteľností vo webovom prehliadači Microsoft Edge.

Štyri vysoko závažné zraniteľnosti dovoľujú neautorizovanému útočníkovi vzdialene vykonávať škodlivý kód. Pre ich úspešné zneužitie potrebuje presvedčiť obeť, aby vykonala úkony na podvrhnutej škodlivej webstránke, ktoré aktivujú funkciu automatického dopĺňania. Zraniteľnosť CVE-2026-66323 spočíva v nevhodnom spôsobe neutralizácie nešpecifikovaného parametru. Chyba zabezpečenia CVE-2026-66798 spočíva v možnosti opätovného použitia dealokovaného miesta v pamäti. CVE-2026-70339 súvisí so zámenou typu premennej a CVE-2026-72970 s pretečení vyrovnávacej pamäte na halde.

Vysoko závažná zraniteľnosť CVE-2026-66324 vyplýva z možnosti externe kontrolovať názov súboru a cestu. Neautorizovaný útočník ju môže zneužiť na vykonávanie spoofingových útokov. Pre je úspešné zneužitie potrebuje presvedčiť obeť, aby vykonala úkony na podvrhnutej škodlivej webstránke, ktoré aktivujú funkciu automatického dopĺňania.

Vysoko závažná zraniteľnosť CVE-2026-72984 spočíva v zámene typu premennej. Neautorizovaný útočník ju môže zneužiť na vzdialené vykonanie škodlivého kódu. Pre je úspešné zneužitie potrebuje presvedčiť obeť, aby navštívila špeciálne vytvorenú webstránku, ktorá zneužije vykresľovací proces prehliadača pre vykonanie kódu.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft Edge (Chromium-based) verzie staršie ako 152.0.7977.64/.65

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-2026-66323
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-66324
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-66798
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70339
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72970
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72984

MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci august opravila 20 vysoko závažných zraniteľností v líniách internetových prehliadačov Firefox, Firefox ESR a Firefox for Android.

Produkty Firefox for Android a Firefox Focus for Android obsahujú zraniteľnosť CVE-2026-18809, ktorá umožňuje získať prístup k neverejným informáciám.

Línia Firefox obsahuje vysoko závažnú zraniteľnosť CVE-2026-75874 v komponente Remote Settings Client, ktorá umožňuje **únik zo sandboxu**.

CVE-2026-74942 sa nachádza v komponente Remote Settings Client línií Firefox a Firefox ESR. Útočníkom umožňuje **eskaláciu oprávnení**.

Línie Firefox a Firefox ESR obsahujú tri zraniteľnosti v komponente Graphics: CanvasWebGL. Chyba zabezpečenia CVE-2026-74934 súvisí s chybami v izolácii stránok. Zraniteľnosť CVE-2026-74941 umožňuje **eskaláciu oprávnení**. Chyba CVE-2026-74946 vyplýva z nesprávne stanovených hraničných podmienok a umožňuje **eskaláciu oprávnení**.

Chyba zabezpečenia CVE-2026-74935 línií Firefox a Firefox ESR v komponente DOM: Networking umožňuje **eskaláciu oprávnení**.

Komponent JavaScript: WebAssembly obsahuje vysoko závažnú zraniteľnosť CVE-2026-74936, ktorá dovoľuje opätovné použitie dealokovanej pamäte. Nachádza sa v líniách Firefox a Firefox ESR.

V komponente JavaScript: GC sa nachádzajú dve vysoko závažné zraniteľnosti. CVE-2026-74937 súvisí s opätovným použitím dealokovanej pamäte a CVE-2026-74938 umožňuje **obísť nešpecifikovanú mitigáciu**. Nachádzajú sa v líniách Firefox a Firefox ESR.

Línie Firefox a Firefox ESR obsahujú vysoko závažnú zraniteľnosť CVE-2026-74939 v komponente DOM: Navigation. Jej zneužitie môže viesť ku **eskalácii oprávnení** útočníka.

Línie Firefox a Firefox ESR obsahujú dve zraniteľnosti v komponente Graphics: Text. CVE-2026-74940 súvisí s opätovným použitím dealokovanej pamäte. CVE-2026-74945 umožňuje získať **prístup k neverejným informáciám**.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť CVE-2026-74943, ktorá dovoľuje opätovné použitie dealokovanej pamäte. Chyba zabezpečenia sa nachádza v komponente Graphics: ImageLib.

Komponent DOM: Core & HTML obsahuje vysoko závažnú zraniteľnosť CVE-2026-74944 vyplývajúcu z možnosti opätovného použitia dealokovanej pamäte. Chyba zabezpečenia je prítomná s líniách Firefox, aj Firefox ESR.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť CVE-2026-74947, ktorá súvisí s neplatným ukazovateľom v pamäti, čo umožňuje **eskaláciu oprávnení**. Obsahujú tiež CVE-2026-74948, ktorá umožňuje získať **prístup k neverejným informáciám**. Chyby zabezpečenia sa nachádzajú v komponente Graphics.

Identifikátory CVE-2026-74987, CVE-2026-74988 a CVE-2026-74990 v líniách Firefox a Firefox ESR opisujú interne objavené sady chýb pri narábaní s pamäťou a iné bezpečnostné chyby, ktoré by podľa spoločnosti Mozilla mohli byť zneužiteľné.

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox verzie staršej ako 154
- Mozilla Firefox ESR verzie staršej ako 115.39, 140.14 a 153.1
- Mozilla Firefox for Android staršej ako 153.0.3

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 154, Firefox ESR na verziu 115.39, 140.14 alebo 153.1 a Firefox for Android aspoň na verziu 153.0.3.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-73/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-74/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-75/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-76/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-77/

GOOGLE CHROME

V mesiaci august spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 19 kritických a 120 vysoko závažných zraniteľností.

Komponent ANGLE obsahuje dve kritické zraniteľnosti. CVE-2026-19157 dovoľuje zapisovať do pamäte mimo povolené hodnoty a CVE-2026-79282 umožňuje opätovne použiť dealokovanú pamäť.

Štyri kritické zraniteľnosti boli opravené v komponente Aura. Chyby zabezpečenia CVE-2026-19149, CVE-2026-79290, CVE-2026-79052 a CVE-2026-79200 vyplývajú z možnosti opätovného použitia dealokovaného miesta v pamäti.

Komponent Dawn obsahuje jednu kritickú zraniteľnosť. CVE-2026-76036 súvisí s pretečením nešpecifikovanej vyrovnávacej pamäte.

V komponente **Chromecast** sa nachádzajú tri kritické zraniteľnosti. CVE-2026-79054 a CVE-2026-79224 dovoľujú opätovne použiť dealokovanú pamäť. CVE-2026-79121 vyplýva z nedostatočného overovania vstupov.

Komponent **Chromoting** obsahuje kritickú zraniteľnosť CVE-2026-76017, ktorá umožňuje opätovné použitie dealokovanej pamäte.

Kritická chyba komponentu **Mobile** s označením CVE-2026-78935 dovoľuje použitie neinicializovanej premennej.

Kritická zraniteľnosť CVE-2026-79012 komponentu **Safe Browsing** umožňuje opätovné použitie dealokovanej pamäte. Chybu zabezpečenia rovnakého typu obsahuje aj komponent **Skia**. Dostala označenie CVE-2026-19154.

Dve kritické chyby zabezpečenia v komponente **Views** umožňujú opätovné použitie dealokovanej pamäte. Dostali identifikátory CVE-2026-19172 a CVE-2026-79150.

Tri kritické zraniteľnosti boli opravené v komponente **WebGL**. Chyby zabezpečenia CVE-2026-19137 a CVE-2026-19170 umožňujú opätovné použitie dealokovaného miesta v pamäti a CVE-2026-76034 súvisí s pretečením nešpecifikovanej vyrovnávacej pamäte.

Spoločnosť Google opravila vysoko závažné zraniteľnosti v komponentoch **Accessibility, ANGLE, Animation, Aura, Autofill, Base, Blink, Bluetooth, Browser, Canvas, Codecs, Contextual Tasks, Core, CORS, Crashpad, CrashReporting, CredentialProvider, Dawn, DOM, Extensions, FedCM, FileSystem, GPU, HTML, Chromecast, Chromoting, Import, Linux Toolkit Theming, Translate, Media, Mobile, Navigation, Network, Paint, Passwords, Payments, Performance, Platform, ReadAloud, Resources, Sandbox, Script, Skia, TabStrip, Tint, UI, USB, V8, Views, WebAPKs, WebAppInstalls, WebAuthentication, WebGL, WebRTC, Workers**. Tieto dovoľujú čítať a zapisovať do pamäte mimo povolené hodnoty, použiť dealokovanú pamäť a neinicializované zdroje, súvisia s pretečením medzipamäte na halde, zásobníku či celočíselnej premennej, vyplývajú zo zámeny typu premennej, vzniku súbehu procesov, nevhodnej implementácie nešpecifikovaných prvkov, nedostatočnej validácie nedôveryhodných vstupov. Súvisia s chybami pamäte, autorizácie, výpočtov a zobrazenia, rozpoznávania referencií a nedostatočnej kontrole zdrojov. Umožňujú získavať citlivé informácie a eskalovať oprávnenia.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows verzie staršej ako 152.0.7977.64/.65
- Google Chrome pre Mac verzie staršej ako 152.0.7977.64/.65
- Google Chrome pre Linux verzie staršej ako 152.0.7977.64

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows aspoň na verziu 152.0.7977.64/.65, Mac aspoň na verziu 152.0.7977.64/.65 a Linux aspoň na verziu 152.0.7977.64.

ZDROJE:

- https://chromereleases.googleblog.com/2026/08
- https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_01193673229.html
- https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_01815628406.html
- https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0826575033.html
- https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0404570826.html
- https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html

4. ADOBE ACROBAT A READER

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

ZDROJE:

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

5. FRAMEWORKY

MICROSOFT .NET FRAMEWORK

V mesiaci august spoločnosť Microsoft opravila 13 vysoko závažných zraniteľností vo frameworku .NET.

Vysoko závažné zraniteľnosti spočívajú v možnosti zápisu do pamäte mimo povolené hodnoty, opätovného použitia dealokovanej pamäte, nevhodnom autorizácie, nedostatočnej kontroly vstupov a dát, či v zlyhaní bezpečnostných mechanizmov. Súvisia s pretečením celočíselnej premennej, vyrovnávacej pamäte na halde, či s možnosťou prechádzania relatívnymi cestami. Vyplývajú z nekonzistentnej interpretácie požiadaviek HTTP či nevhodného spôsobu narábania s informáciami. Väčšinu z nich môže zneužiť vzdialený útočník bez oprávnení. Umožňujú mu **navýšiť svoje oprávnenia, vzdialene vykonávať kód, obchádzať bezpečnostné prvky, 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 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
- 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

ORACLE JAVA

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

ZDROJE:

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

INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

RUBY ON RAILS ACTIVE STORAGE: KRITICKÁ ZRANITEĽNOSŤ UMOŽŇUJE ČÍTANIE OBSAHU SÚBOROV S POTENCIÁLOM VZDIALENÉHO VYKONANIA KÓDU

V komponente Active Storage nástroja Ruby on Rails bola opravená kritická zraniteľnosť CVE-2026-66066, ktorá umožňuje neautentifikovanému útočníkovi čítať ľubovoľné súbory zo servera prostredníctvom špeciálne vytvoreného obrázka. Získané citlivé údaje, napríklad kryptografické kľúče, prihlasovacie údaje k databázam alebo kľúče k aplikačnému programového rozhraniu (API), môžu následne umožniť kompromitáciu aplikácie alebo v určitých prípadoch viesť až k vzdialenému vykonaniu kódu. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI VMWARE VCENTER

Spoločnosť Broadcom opravila v produkte VMware vCenter dve kritické zraniteľnosti, z ktorých jedna je aktívne zneužívaná. Zraniteľnosti umožňujú vzdialeným neautentifikovaným útočníkom

obchádzať autentifikáciu a traverzovať adresármi s cieľom vykonávania ľubovoľného kódu. Viac informácií na stránke.

ZRANITEĽNOSŤ FORTIWEB UMOŽŇUJE PRIHLÁSIŤ SA ĽUBOVOĽNÝMI ÚDAJMI

Spoločnosť Fortinet opravila kritickú zraniteľnosť vo svojom produkte FortiWeb, ktorá umožňuje vzdialenému útočníkovi prihlásiť sa do administrátorskej konzoly s použitím ľubovoľného prihlasovacieho mena a hesla. Viac informácií na stránke.

ZRANITEĽNOSTI GITLAB CE/EE DOVOĽUJÚ UPRAVOVAŤ A MENIŤ PROJEKTY A DÁTA

Vývojári platformy GitLab CE/EE opravili dve zraniteľnosti v komponente GraphQL, ktoré umožňujú vzdialeným neautentifikovaným útočníkom meniť a mazať verejné projekty a používateľské dáta. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ RED HAT BUILD OF KEYCLOAK UMOŽŇUJE JEDNODUCHÉ PREVZATIE ÚČTOV

Spoločnosť Red Hat opravila kritickú zraniteľnosť v komponente keycloak-services. Chyba v procese obnovy prihlasovacích údajov umožňuje neautentizovanému útočníkovi s prístupom k službe vynútiť reset hesla ktoréhokoľvek používateľa bez nutnosti kliknúť na overovací e-mailový odkaz a získať tak plnú kontrolu nad jeho účtom. Viac informácií na stránke.

ZRANITEĽNOSŤ WORDPRESS ELEMENTOR PRO UMOŽŇUJE VYKONÁVAŤ KÓD

Vývojári modulu Elementor Pro pre WordPress opravili kritickú zraniteľnosť, ktorá dovoľuje obchádzať kontrolu zakázaných súborov a nahrávať ich na server. Vzdialený neautentifikovaný útočník tak môže získať schopnosť vykonávať ľubovoľný kód. Viac informácií na stránke.

ORACLE VYDALA BALÍK ZÁPLAT NA 943 ZRANITEĽNOSTÍ VIACERÝCH PRODUKTOV

V augustovom balíku záplat opravila spoločnosť Oracle vo svojich produktoch 943 zraniteľností, vrátane 154 kritických. Viac informácií na stránke.

V NEXT.JS OPRAVILI DVE KRITICKÉ ZRANITEĽNOSTI

Vývojári frameworku Next.js opravili dve kritické zraniteľnosti, ktoré umožňujú neautentifikovaným útočníkom vzdialené vykonávanie kódu. Viac informácií na stránke.