MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

JÚL 2026

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci júl 31 kritických a 371 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritická zraniteľnosť CVE-2026-42982 vo **Windows Secure Kernel Mode** vyplýva z nedostatočnej kontroly nedôveryhodných vstupov a CVE-2026-50392 súvisí s možnosťou použitia dealokovaného priestoru v pamäti. Lokálny útočník s nízkymi oprávneniami ich môže zneužiť na **zvýšenie svojich oprávnení** až na úroveň SYSTEM.

Kritické zraniteľnosti komponentu **DHCP Server Service** vyplývajú z pretečenia vyrovnávacej pamäte na halde a dovoľujú **vzdialené vykonanie kódu**. CVE-2026-48564 vyžaduje aspoň nízke oprávnenia v zraniteľnom systéme a prihlásenie a zneužiť ju možno odoslaním špeciálne vytvoreným volaním RPC. CVE-2026-50370 nevyžaduje žiadne oprávnenia a zneužiť ju možno po prihlásení poslaním špeciálne vytvoreného sieťového obsahu na zraniteľný server. CVE-2026-56159 nevyžaduje oprávnenia ani prihlásenie a zneužiť ju možno zaslaním špeciálne vytvoreného paketu na DHCP server, ktorý posiela odpoveď Option 43. Zraniteľnosť CVE-2026-50518 možno zneužiť bez autorizácie zaslaním špeciálne vytvorených sieťových požiadaviek, ktoré môžu vyvolať poškodenie pamäte.

Kritická zraniteľnosť CVE-2026-54128 v komponente **Windows DHCP Client** súvisí s možnosťou použitia dealokovaného miesta v pamäti. Lokálny neautorizovaný útočník ju môže zneužiť na **vykonanie kódu**.

Kritické zraniteľnosti CVE-2026-49164 a CVE-2026-54121 sa nachádzajú vo **Windows Active Directory Domain Services** a **Active Directory Certificate Services**. Prvá súvisí s pretečením vyrovnávacej pamäte na halde. Útočník bez oprávnení ju môže zneužiť na **vzdialené vykonanie kódu**. Druhá vzniká kvôli nevhodnému autorizačnému mechanizmu a umožňuje vzdialenému útočníkovi s nízkymi oprávneniami **zvýšiť svoje oprávnenia** na úroveň administrátora.

Kritická zraniteľnosť CVE-2026-50444 **Windows Server Update Service (WSUS)** vyplýva z absencie autentifikácie nešpecifikovanej kritickej funkcie. Vzdialený útočník s nízkymi oprávneniami ju môže zneužiť na **zvýšenie svojich oprávnení**.

Kritické zraniteľnosti CVE-2026-49796 a CVE-2026-50380 vo **Windows GDI+** súvisia s pretečením vyrovnávacej pamäte na halde. Útočníkom bez oprávnení umožňujú **vykonávať ľubovoľný kód**, prvá **lokálne**, druhá **vzdialene**. Pre ich úspešné zneužitie môže útočník presvedčiť obeť, aby otvorila špeciálne vytvorený súbor.

Kritická zraniteľnosť CVE-2026-50382 komponentu **DirectX Graphics Kernel** súvisí s dereferenciou nedôveryhodného ukazovateľa. Lokálny útočník s nízkymi oprávneniami ju môže zneužiť na **vykonanie ľubovoľného kódu**. Útočník môže využiť prístup k hosťovskému virtuálnemu stroju na útok na hostiteľský operačný systém.

Kritické zraniteľnosti CVE-2026-50327 a CVE-2026-58542 komponentu **Windows Media** vyplývajú z pretečenia vyrovnávacej pamäte na halde. Lokálny útočník ich môže zneužiť na **vykonanie ľubovoľného kódu**. Prvá vyžaduje nízke oprávnenia, pre zneužitie druhej nie sú potrebné žiadne oprávnenia.

Päť kritických zraniteľností sa nachádza v komponente **Windows Media Foundation**. Zraniteľnosti CVE-2026-50655, CVE-2026-56189, CVE-2026-57087, CVE-2026-57090 a CVE-2026-57094 vyplývajú z pretečenia vyrovnávacej pamäte na halde a neautorizovaný útočník ich môže zneužiť na **vykonanie ľubovoľného kódu**. Prvé dve umožňujú vykonávať kód **lokálne**, ďalšie tri aj **vzdialene**. Pre ich úspešné zneužitie potrebuje útočník interakciu obete.

Kritické zraniteľnosti CVE-2026-50680 a CVE-2026-54127 vo **Windows Hyper-V** súvisia s pretečením vyrovnávacej pamäte na halde a možnosťou opätovného využitia deakolovanej pamäte. Lokálny útočník ich môže zneužiť na **eskalovanie svojich oprávnení**. Prvá vyžaduje vysoké oprávnenia, no umožňuje ich navýšiť až na úroveň SYSTEM. Druhá nevyžaduje žiadne oprávnenia.

Kritická zraniteľnosť sa nachádza aj v komponente **Windows Remote Desktop Client**. CVE-2026-50474 súvisí s možnosťou opätovného využitia deakolovanej pamäte. Zraniteľnosť môže zneužiť neautorizovaný útočník na **vzdialené vykonanie kódu**.

Kritická zraniteľnosť v komponente **Windows Secure Socket Tunneling Protocol (SSTP)**. CVE-2026-50694 súvisí s možnosťou opätovného využitia deakolovanej pamäte. Zraniteľnosť môže zneužiť neautorizovaný útočník na **vzdialené vykonanie kódu**. Potrebuje na to poslať špeciálne vytvorený paket SSTP zraniteľnému SSTP serveru.

Komponent **Windows Reliable Multicast Transport Driver (RMCAST)** obsahuje dve kritické zraniteľnosti, ktoré umožňujú neautorizovaným útočníkom **vzdialene vykonávať kód**. CVE-2026-54982 vyplýva z podtečenia celočíselnej premennej a zneužiť ju možno len z rovnakého segmentu siete, kde sa nachádza zraniteľné zariadenie. CVE-2026-54995 súvisí s možnosťou opätovného využitia deakolovanej pamäte.

Kritická zraniteľnosť CVE-2026-54992 komponentu **Microsoft Message Queuing Queue Manager** vyplýva z pretečenia vyrovnávacej pamäte na halde. Lokálny neautorizovaný útočník ju môže zneužiť na **vykonanie ľubovoľného kódu**.

Komponent **Windows TCP/IP obsahuje** kritickú zraniteľnosť CVE-2026-54999, ktorá umožňuje neautorizovaným útočníkom **vzdialene vykonávať kód** z rovnakého segmentu siete, kde sa nachádza zraniteľné zariadenie. Chyba zabezpečenia súvisí so vznikom súbehu a využívania zdieľaného zdroja bez vhodnej synchronizácie.

Podobná kritická chyba označená ako CVE-2026-56188 sa nachádza v ovládači **Windows Server Network**. Súvisí so vznikom súbehu a využívania zdieľaného zdroja bez vhodnej synchronizácie. Neautorizovaným útočníkom dovoľuje **vzdialene vykonávať kód** zaslaním špeciálne vytvoreného sieťového obsahu zraniteľnému serveru.

Kritická zraniteľnosť CVE-2026-57092 v **Microsoft Windows VMSwitch** vyplýva z možnosti opätovného použitia deakolovanej pamäte. Vzdialený útočník s nízkymi oprávneniami na virtuálnom stroji ju môže zneužiť na **zvýšenie svojich oprávnení** na hostiteľskom systéme.

Kritická zraniteľnosť CVE-2026-58608 v komponente **Windows Print Spooler** súvisí s možnosťou použitia dealokovaného miesta v pamäti a so vznikom súbehu. Útočník s nízkymi oprávneniami ju môže zneužiť na **vzdialené vykonanie kódu**. Môže otvoriť handle tlačiarne, ktorú zatvorí bez zneplatnenia pridruženej notifikačnej handle.

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:

- Microsoft Configuration Manager 2509
- Microsoft Configuration Manager 2603
- Remote Desktop Web Client
- 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 Admin Center
- 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-2026-42982
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-48564
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-49164
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-49796
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50327
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50370
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50380
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50382
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50392

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50444
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50474
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50518
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50655
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50680
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50694
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-54121
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-54127
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-54128
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-54982
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-54992
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-54995
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-54999
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56159
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56188
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56189
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-57087
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-57090
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-57092
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-57094
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58542
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58608

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 júl bezpečnostné aktualizácie, ktoré opravujú 22 kritických a 83 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritické zraniteľnosti CVE-2026-50314, CVE-2026-50467 a CVE-2026-55018 balíkov **Microsoft Office** vyplývajú z možnosti opätovného použitia dealokovaného miesta v pamäti. Neautorizovaný útočník ich môže zneužiť na **lokálne vykonanie ľubovoľného kódu**. Potrebuje k tomu presvedčiť obeť, aby otvorila škodlivý súbor MS Office. Útočným vektorom pre zneužitie zraniteľností môže byť aj náhľad dokumentu (Preview Pane).

Kritická zraniteľnosť CVE-2026-55022 balíkov **Microsoft Office** umožňuje neautorizovanému útočníkovi **lokálne vykonávať ľubovoľný kód**. Vyplýva zo zámeny typu premennej. Pre jej zneužitie musí presvedčiť obeť, aby otvorila špeciálne pripravený súbor MS Office. Útočným vektorom pre zneužitie tejto zraniteľnosti môže byť aj náhľad dokumentu (Preview Pane).

Kritická zraniteľnosť CVE-2026-55045 balíkov **Microsoft Office** umožňuje neautorizovanému útočníkovi **lokálne vykonávať ľubovoľný kód** bez interakcie obete. Súvisí s možnosťou čítania pamäte mimo povolené hodnoty. Útočným vektorom pre zneužitie tejto zraniteľnosti môže byť aj náhľad dokumentu (Preview Pane).

Balíky **Microsoft Office** obsahujú aj štyri kritické zraniteľnosti CVE-2026-55049, CVE-2026-55056, CVE-2026-55129 a CVE-2026-55140, ktoré vyplývajú z pretečenie vyrovnávacej pamäte na halde. Neautorizovaný útočník ich môže zneužiť na **lokálne vykonanie ľubovoľného kódu**. Potrebuje k tomu presvedčiť obeť, aby otvorila škodlivý súbor MS Office. Útočným vektorom pre zneužitie zraniteľností môže byť aj náhľad dokumentu (Preview Pane).

Kritické zraniteľnosti **Microsoft SharePoint** s označením CVE-2026-50522 a CVE-2026-58644 môže neautorizovaný útočník zneužiť na **vzdialené vykonanie ľubovoľného kódu**. Chyby zabezpečenia vyplývajú z neošetrenej deserializácie nedôveryhodných údajov. Chyba zabezpečenia CVE-2026-58644 je **aktívne zneužívaná**.

Microsoft SharePoint Server obsahuje kritickú zraniteľnosť s označením CVE-2026-55040, ktorú môže vzdialený neautorizovaný útočník zneužiť na **obídenie autentifikácie** na zraniteľnej inštancii SharePoint Server. Chyba zabezpečenia vyplýva z nedostatočného overovania totožnosti v rámci autentifikačného procesu. Útočník môže po úspešnom zneužití zraniteľnosti získať prístup ku súborom a dátam, ktoré môže aj modifikovať.

V **Microsoft Word** boli opravené tri kritické zraniteľnosti, ktoré môže neautorizovaný útočník zneužiť na **lokálne vykonanie ľubovoľného kódu**. CVE-2026-55033 je spôsobená pretečením vyrovnávacej pamäte na halde a celočíselnej premennej, CVE-2026-55127 súvisí s pretečením vyrovnávacej pamäte na halde a CVE-2026-55132 vyplýva z dvojitého uvoľnenia pamäte. Pre ich zneužitie musí útočník presvedčiť obeť, aby otvorila špeciálne pripravený súbor MS Office. Útočným vektorom pre zneužitie zraniteľností môže byť aj náhľad dokumentu (Preview Pane).

Tri kritické zraniteľnosti boli opravené aj v **Microsoft PowerPoint**. Neautorizovaný útočník ich môže zneužiť na **lokálne vykonanie ľubovoľného kódu**. CVE-2026-55043 je spôsobená pretečením vyrovnávacej pamäte na halde a celočíselnej premennej, CVE-2026-55120 súvisí s pretečením vyrovnávacej pamäte na halde a CVE-2026-55123 vyplýva z pretečenia vyrovnávacej pamäte na halde a nesprávnej konverziou typov číselných premenných. Pre ich zneužitie musí útočník presvedčiť obeť, aby otvorila špeciálne pripravený súbor MS Office.

Kritickú zraniteľnosť 2026-58275 v produkte **Azure DNS** a CVE-2026-62825 v produkte **Azure Key Vault** opravila spoločnosť Microsoft na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre ich odstránenie. Zraniteľnosti môže neautorizovaný vzdialený útočník zneužiť na **zvýšenie svojich oprávnení**. Chyby zabezpečenia súvisia s absentujúcim mechanizmom autorizácie a nevhodným spôsobom autentifikácie.

Dve kritické zraniteľnosti **Microsoft 365 Copilot** opravila spoločnosť Microsoft na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre ich odstránenie. Zraniteľnosť s označením CVE-2026-41106 môže neautorizovaný vzdialený útočník zneužiť na **zvýšenie svojich oprávnení**. Chyba zabezpečenia súvisí s 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**.

Vysoko závažné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu, navýšenie privilégií, získavanie citlivých informácií** a **spoofingové útoky**.

ZRANITEĽNÉ SYSTÉMY:

- Azure DNS
- Azure Key Vault
- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft 365 Copilot
- Microsoft 365 Copilot for iOS
- Microsoft Bing Search for iOS
- Microsoft Excel 2016 (32-bit edition)
- Microsoft Excel 2016 (64-bit edition)
- Microsoft Office 2016 (32-bit edition)
- Microsoft Office 2016 (64-bit edition)
- Microsoft Office 2019 for 32-bit editions
- Microsoft Office 2019 for 64-bit editions
- Microsoft Office 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 PC Manager
- Microsoft PowerPoint 2016 (32-bit edition)
- Microsoft PowerPoint 2016 (64-bit edition)
- Microsoft SharePoint Enterprise Server 2016

- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription Edition
- Microsoft Word 2016 (32-bit edition)
- Microsoft Word 2016 (64-bit edition)
- Office Online Server
- Windows Terminal App
- Windows Terminal for Windows 10
- Windows Terminal for Windows 11

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-2026-41106
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50314
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50467
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50517
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50522
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55018
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55022
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55033
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55040
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55043
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55045
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55049
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55056
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55120
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55123

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55127
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55129
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55132
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55140
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58275
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58644
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62825

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 júl opravila 46 vysoko závažných zraniteľností vo webovom prehliadači Microsoft Edge.

Vysoko závažné zraniteľnosti spočívajú v možnosti opätovného použitia dealokovaného miesta v pamäti, zámene typu premennej, deserializácii nedôveryhodných vstupov, dereferencii nedôveryhodného ukazovateľa, pretečení vyrovnávacej pamäte na halde alebo celočíselnej premennej, nevhodnej kontrole prístupov, nevhodnom spôsobe ošetrenia nedôveryhodných vstupov, neošetrenom SSRF, nevhodnom mechanizme prideľovania autorizácie, v možnosti traverzovania cestami a použitia už uvoľnených zdrojov, vo vzniku súbehov, či exponovaní citlivých informácií a súborov nepovolaným používateľom. Útočníkom umožňujú vzdialené

vykonanie škodlivého kódu, navýšenie privilégií, získavanie citlivých informácií, obchádzanie bezpečnostných prvkov, zasahovanie do systému a spoofingové útoky.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft Edge (Chromium-based) verzie staršie ako 150.0.4078.99

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

MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci júl opravila 2 kritické a 21 vysoko závažných zraniteľností v líniách internetových prehliadačov Firefox a Firefox ESR.

Línie Firefox a Firefox ESR obsahujú kritickú zraniteľnosť CVE-2026-15718 v komponente JavaScript: WebAssembly, ktorá súvisí s neplatným ukazovateľom. Pre zraniteľnosť existuje verejne dostupný exploit.

Línie Firefox a Firefox ESR obsahujú kritickú zraniteľnosť CVE-2026-15719 v komponente DOM: Navigation, ktorá súvisí s mechanizmom izolácie stránok. Pre zraniteľnosť existuje verejne dostupný exploit.

Komponent DOM: Navigation obsahuje tri vysoko závažné zraniteľnosti. CVE-2026-16349 umožňuje obchádzať politiku same-origin, CVE-2026-16351 umožňuje únik zo sandboxu kvôli chybe dovoľujúcej opätovné použitie dealokovanej pamäte a zneužitie CVE-2026-16366 môže viesť ku eskalácii oprávnení.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť CVE-2026-16350, ktorá súvisí s nesprávne nastavenými hraničnými podmienkami. Chyba zabezpečenia sa nachádza v komponente Audio/Video: cubeb.

Línia Firefox obsahuje chybu zabezpečenia CVE-2026-16364, ktorá súvisí s nesprávne nastavenými hraničnými podmienkami. Nachádza sa v komponente Audio/Video: Playback.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť CVE-2026-16362, ktorá umožňuje opätovné použitie dealokovanej pamäte. Chyba zabezpečenia sa nachádza v komponente WebRTC: Audio/Video.

Zraniteľnosti komponentu Disability Access APIs CVE-2026-16352 a CVE-2026-16356 v líniách Firefox a Firefox ESR a CVE-2026-16367 v línii Firefox umožňujú **únik zo sandboxu** kvôli chybe dovoľujúcej opätovné použitie dealokovanej pamäte.

Vysoko závažná zraniteľnosť CVE-2026-16353 sa nachádza v komponente DOM: Bindings (WebIDL) a súvisí s neplatným ukazovateľom v pamäti. Zasahuje línie Firefox a Firefox ESR.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť CVE-2026-16354, ktorá umožňuje získať **prístup k neverejným informáciám**. Chyba zabezpečenia sa nachádza v komponente Graphics: ImageLib.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť CVE-2026-16355 v komponente JavaScript Engine: JIT a CVE-2026-16363 v JavaScript: WebAssembly, ktoré spôsobujú nesprávnu kompiláciu.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť CVE-2026-16357, ktorá súvisí s nesprávne nastavenými hraničnými podmienkami. Chyba zabezpečenia sa nachádza v komponente Graphics.

Línia Firefox obsahuje chybu zabezpečenia, ktorá umožňuje **eskaláciu oprávnení**. Zraniteľnosť CVE-2026-16365 sa nachádza v komponente DOM: Workers.

Komponent JavaScript: WebAssembly obsahuje dve vysoko závažné zraniteľnosti. CVE-2026-16368 súvisí s nesprávne nastavenými hraničnými podmienkami a CVE-2026-16369 s pretečením celočíselnej premennej.

Identifikátor CVE-2026-16411 v línii Firefox, CVE-2026-16361 vo Firefox ESR a identifikátory CVE-2026-16412 a CVE-2026-16360 v líniách Firefox a Firefox ESR opisujú sady chýb pri narábaní s pamäťou. Tieto zraniteľnosti ovplyvňujú bezpečnosť pamäte a môžu viesť ku **poškodeniu pamäte** alebo možnosti **vykonávať kód**.

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox verzie staršej ako 153
- Mozilla Firefox ESR verzie staršej ako 115.38 a 140.13

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 153 a Firefox ESR na verziu 115.38 alebo 140.13.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-67/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-68/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-69/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-70/

GOOGLE CHROME

V mesiaci júl spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 14 kritických a 122 vysoko závažných zraniteľností.

Komponent **ANGLE** obsahuje kritickú zraniteľnosť CVE-2026-17655, ktorá súvisí s nedostatočnou kontrolou nedôveryhodných vstupov.

Kritická chyba zabezpečenia CVE-2026-15899 sa nachádza v komponente **CameraCapture** a umožňuje opätovne použiť dealokovanú pamäť. Rovnaká kritická zraniteľnosť sa nachádza v komponente **Composing**. Dostala identifikátor CVE-2026-17650.

Komponent **Dawn** obsahuje jednu kritickú zraniteľnosť. CVE-2026-17651 súvisí s nedostatočnou kontrolou nedôveryhodných vstupov.

Kritická chyba komponentu **GPU** s označením CVE-2026-15900 dovoľuje opätovné použitie dealokovaného miesta v pamäti. V komponente **Network** bola opravená rovnakej kategórie s označením CVE-2026-15901.

Štyri kritické zraniteľnosti boli opravené v komponente **Ozone**. Chyby zabezpečenia CVE-2026-15112, CVE-2026-15764, CVE-2026-15765 a CVE-2026-17656 vyplývajú z možnosti opätovného použitia dealokovaného miesta v pamäti.

Komponent **Skia** obsahuje kritickú zraniteľnosť CVE-2026-17653, ktorá umožňuje opätovné použitie dealokovanej pamäte.

Kritická zraniteľnosť CVE-2026-17654 komponentu **Updater** súvisí so vznikom súbehu.

Dve kritické chyby zabezpečenia v komponente **Views** umožňujú opätovné použitie dealokovanej pamäte. Dostali identifikátory CVE-2026-15129 a CVE-2026-17652.

Spoločnosť Google opravila vysoko závažné zraniteľnosti v komponentoch **Accessibility, Actor, ANGLE, Audio, Aura, Autofill, Blink, Cast, Certificate, Codecs, Color, Core, DataTransfer, DOM, Downloads, Enterprise, Extensions, FileSystem, Forms, GetUserMedia, GPU, HTML, HTML-in-Canvas, Chrome for iOS, Chromecast, Input, InterestGroups, libyuv, libxml, Linux Toolkit Theming, Loader, Media, MHTML, Navigation, Network, Ozone, Passwords, Payments, PDF, Prefetch, Print Preview, QUIC, SiteIsolation, Skia, UI, Updater, V8, Views, WebAppInstalls, WebAudio, WebAuthentication, WebGL, WebMCP, WebRTC, WebView**. 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, nedostatočného presadzovania nešpecifikovaných politík a nedostatočnej validácie dát a nedôveryhodných vstupov. Súvisia s chybami v životnom cykle objektov, kryptografickej ochrane a umožňujú získavať informácie bočnými kanálmi.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows verzie staršej ako 151.0.7922.71/.72
- Google Chrome pre Mac verzie staršej ako 151.0.7922.71/.72
- Google Chrome pre Linux verzie staršej ako 151.0.7922.71

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows aspoň na verziu 151.0.7922.71/.72, Mac aspoň na verziu 151.0.7922.71/.72 a Linux aspoň na verziu 151.0.7922.71.

ZDROJE:

- https://chromereleases.googleblog.com/2026/07
- https://chromereleases.googleblog.com/2026/07/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2026/07/stable-channel-update-for-desktop_01162222768.html

- https://chromereleases.googleblog.com/2026/07/stable-channel-update-for-desktop_0353146366.html
- https://chromereleases.googleblog.com/2026/07/stable-channel-update-for-desktop_049796704.html
- https://chromereleases.googleblog.com/2026/07/stable-channel-update-for-desktop_0256605430.html
- https://chromereleases.googleblog.com/2026/07/stable-channel-update-for-desktop_01320465736.html
- https://chromereleases.googleblog.com/2026/07/stable-channel-update-for-desktop_0887107924.html

4. ADOBE ACROBAT A READER

V mesiaci júl 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 júl spoločnosť Microsoft opravila 27 vysoko závažných zraniteľností vo frameworku .NET.

Vysoko závažné zraniteľnosti spočívajú v zámene typu premennej, nevhodnom spôsobe autentifikácie a autorizácie, nedostatočnej sanitizácii vstupov, deserializácii nedôveryhodných dát, či v nevhodnom spôsobe overovania kryptografických podpisov. Súvisia s pretečením vyrovnávacej pamäte zásobníka, vzniku nekonečnej slučky, či s nevhodným spôsobom narábania s odkazmi pred prístupom ku súborom. Vyplývajú z nevhodnej kontroly generovania kódu a z absentujúceho obmedzenia využívania výpočtových zdrojov. Väčšinu z nich môže zneužiť vzdialený útočník bez oprávnení. Umožňujú mu navýšiť svoje oprávnenia, vzdialene

vykonávať kód, obchádzať bezpečnostné prvky, vykonávať spoofingové útoky a zásahy do systému 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 4.7.2
- 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
- Microsoft.AspNet.OData
- Microsoft.AspNetCore.OData

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 v mesiaci júl vydala bezpečnostné aktualizácie, ktoré opravujú 5 vysoko závažných zraniteľností v rámci Oracle Java SE.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2026-62574 sa nachádza v komponente Install. Lokálny útočník s nízkymi oprávneniami by ju mohol zneužiť pre **získanie kontroly nad zraniteľnou aplikáciou**.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2026-47057 sa nachádza v komponente Scripting. Neautentifikovaný vzdialený útočník by ju mohol zneužiť pomocou API a spôsobiť opakovaný **pád aplikácie (DoS)**. Druhá zraniteľnosť komponentu Scripting dostala identifikátor CVE-2026-47058 a vzdialenému neautentifikovanému útočníkovi dovoľuje pomocou volaní API získať možnosť **vytvárať, modifikovať a mazať údaje**, vrátane kritických dát.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2026-41254 sa nachádza v komponente 2D (Little CMS), v CubeSize v súbore cmslut.c. Súvisí s pretečením celočíselnej premennej kvôli nesprávne nastaveným kontrolám. Zneužiť ju môže neautentifikovaný vzdialený útočník.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2026-47063 sa nachádza v komponente Libraries. Neautentifikovaný vzdialený útočník by ju mohol zneužiť pomocou volaní API a získať možnosť **vytvárať, modifikovať a mazať údaje**, vrátane kritických dát.

ZRANITEĽNÉ SYSTÉMY:

- Oracle Java SE: 8u491, 8u491-perf, 11.0.31, 17.0.19, 21.0.11, 25.0.3, 26.0.1
- Oracle GraalVM for JDK: 17.0.19, 21.0.11
- GraalVM Enterprise Edition: 21.3.18

ODPORÚČANIA:

Odporúčame aktualizovať zraniteľné verzie Java SE na aktuálne verzie prostredníctvom Java Auto Update alebo na stránke spoločnosti Oracle, ktorú môžete nájsť v časti zdroje.

ZDROJE:

- https://www.oracle.com/security-alerts/
- https://www.oracle.com/security-alerts/cpujul2026.html#AppendixJAVA
- https://nvd.nist.gov/vuln/detail/CVE-2026-62574

- https://nvd.nist.gov/vuln/detail/CVE-2026-47057
- http://nvd.nist.gov/vuln/detail/CVE-2026-41254
- http://nvd.nist.gov/vuln/detail/CVE-2026-47058
- https://nvd.nist.gov/vuln/detail/CVE-2026-47063

INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

DIRTYCLONE: ZRANITEĽNOSŤ JADRA LINUXU UMOŽŇUJE ZÍSKAŤ PRÁVA ROOT

V jadre operačných systémov Linux bola opravená vysoko závažná zraniteľnosť, ktorá umožňuje lokálnym útočníkom s nízkymi oprávneniami vykonávať zmeny v pamäte pomocou klonovaných sieťových paketov a získať oprávnenia používateľa root. Chyba zabezpečenia patrí do sady chýb DirtyFrag a dostala názov DirtyClone. Viac informácií na stránke.

JANUSCAPE: ZRANITEĽNOSŤ LINUXOVÉHO HYPERVÍZORA KVM UMOŽŇUJE UNIKNÚŤ NA HOSTITEĽA

Hypervízor KVM pre Linux obsahuje zraniteľnosť, ktorá útočníkom s prístupom ku vitruálnemu stroju a s oprávneniami používateľa root umožňuje spôsobiť kernel panic na hostiteľovi (DoS), a v istých prípadoch tiež na hostiteľovi vykonávať kód s oprávneniami root. Zraniteľné sú najmä multi-tenantné cloudové systémy s vnorenou virtualizáciou. Viac informácií na stránke.

ROUTERY TENDA OBSAHUJÚ ZADNÉ VRÁTKA DO ADMINISTRÁTORSKÉHO ROZHRANIA

Tím CERT/CC objavil zadné vrátka vo firmvéri smerovačov Tenda, ktoré umožňujú zadať alternatívne predkonfigurované heslo bez znalosti používateľského mena, a získať administrátorský prístup ku zariadeniu. Táto funkcia nie je zdokumentovaná, ani viditeľná v administrátorskom rozhraní. Viac informácií na stránke.

UBIQUITI OPRAVILA KRITICKÉ ZRANITEĽNOSTI V UNIFI CONNECT, UNIFI TALK, UNIFI ACCESS, UNIFI PROTECT A UNIFI OS

Spoločnosť Ubiquiti vydala bezpečnostné aktualizácie, ktoré riešia 25 kritických a vysoko závažných bezpečnostných zraniteľností ovplyvňujúcich UniFi Connect, UniFi Talk, UniFi Access,

UniFi Protect a UniFi OS. Kritické chyby umožňujú eskaláciu privilégií a vykonávanie ľubovoľných príkazov. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ ZIMBRA CLASSIC WEB CLIENT

Vývojári mailového klienta Zimbra Classic Web Client opravili kritickú chybu, ktorá umožňuje vykonávať útoky typu XSS a týmto spôsobom vykonávať kód v zariadení obetí. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI ROZŠÍRENÍ JOOMLA, ICAGENDA A BALBOOA FORMS, UMOŽŇUJÚ VYKONÁVAŤ KÓD

Vývojári rozšírení iCagenda a Balbooa Forms pre redakčný systém Joomla opravili kritické zraniteľnosti, ktoré umožňujú nahrávať na webserver súbory s ľubovoľnými príponami, čo môže viesť ku vzdialenému vykonaniu kódu PHP, alebo iného kódu pod kontrolou útočníka. Viac informácií na stránke.

ZRANITEĽNOSTI RABBITMQ UMOŽŇUJÚ ZÍSKAVAŤ INFORMÁCIE A ADMINISTRÁTORSKÝ TOKEN

Vývojári message brokera RabbitMQ opravili dve zraniteľnosti, ktoré umožňujú neautentifikovaným útočníkom získať klientske tajomstvo OAuth a cez neho administrátorský token, alebo vykonávať zber informácií o prebiehajúcej komunikácii. Viac informácií na stránke.

SAP OPRAVIL V JÚLI KRITICKÉ ZRANITEĽNOSTI V NETWEAVER, APPROUTER A COMMERCE CLOUD

Spoločnosť SAP vydala bezpečnostné aktualizácie svojich systémov, ktoré opravujú 17 zraniteľností. V SAP NetWeaver, SAP Approuter a SAP Commerce Cloud boli opravené 4 chyby zabezpečenia označené ako kritické. Viac informácií na stránke.

ZNEUŽÍVANÁ KRITICKÁ ZRANITEĽNOSŤ ORACLE EBS PAYMENTS

Spoločnosť Oracle opravila kritickú zraniteľnosť v aplikácii Oracle Payments, ktorá je súčasťou E-Business Suite. Neautentifikovaný útočník ju môže zneužiť pre získanie kontroly nad aplikáciou. Zraniteľnosť je aktívne zneužívaná. Viac informácií na stránke.

ZRANITEĽNOSTI PRODUKTOV ZOOM PRE WINDOWS UMOŽŇUJÚ NAVÝŠIŤ OPRÁVNENIA A PREVZIAŤ ÚČTY

Spoločnosť Zoom vydala aktualizácie pre kritickú zraniteľnosť v Zoom Workplace pre Windows. CVE-2026-53412 môže neautentifikovanému útočníkovi umožniť prevziať používateľský účet. Zároveň opravila tri vysoko závažné zraniteľnosti, ktoré umožňujú získať vyššie oprávnenia a zasahujú niektoré ďalšie produkty. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ F5 NGINX PLUS A NGINX OPEN SOURCE UMOŽŇUJE VYKONÁVAŤ KÓD

Spoločnosť F5 opravila kritickú zraniteľnosť v produktoch NGINX Plus a NGINX Open Source, ktorá umožňuje vzdialeným neautentifikovaným útočníkom pomocou HTTP dopytov získavať informácie o ukazovateľoch v pamäti a vykonávať tak kód, alebo spôsobiť reštart systému. Viac informácií na stránke.

ZRANITEĽNOSŤ OPENSSL UMOŽŇUJE EFEKTÍVNE VYČERPAŤ PAMÄŤ SERVERA

Vývojári knižnice OpenSSL opravili závažnú zraniteľnosť, ktorá umožňuje zahltiť pamäť servera odosielaním hlavičiek TLS handshake o veľkosti 11B s požiadavkou alokovať až 131KB. Chyba vyplýva za spôsobu, akým OpenSSL spracúva požiadavky na alokovanie pamäte pre telá správ. Viac informácií na stránke.

V JADRE LINUXU BOLO OPRAVENÝCH 442 ZRANITEĽNOSTÍ

Vývojári linuxového jadra opravili v novej verzii 442 zraniteľností, z ktorých 57 dostalo hodnotenie kritická a 211 vysoko závažná. Zraniteľnosti ovplyvňovali správu sietí, narábanie so súborovým systémom a pamäťou, Bluetooth, virtualizáciu, ovládače a bezpečnostné prvky. Viac informácií na stránke.

ZRANITEĽNOSŤ 7-ZIP UMOŽŇUJE VYKONÁVAŤ ĽUBOVOĽNÝ KÓD

Vývojári populárneho archivátora 7-Zip opravili vysoko závažnú zraniteľnosť vo funkcionalite pre narábanie s archívmi XZ. Chyba zabezpečenia umožňuje neautorizovaným útočníkom podvrhnúť obeti špeciálne upravený súbor, po ktorého otvorení dôjde ku vykonaniu ľubovoľného kódu. Viac informácií na stránke.

V Zimbra Collaboration Suite bolo opravených deväť kritických zraniteľností

Vývojári Zimbra Collaboration Suite opravili 9 kritických zraniteľností, ktoré umožňujú vzdialene vykonávať príkazy cez útoky XSS alebo zneužitím implementácie SNMP. Jedna zraniteľnosť umožňuje obísť reštrikcie preposielania e-mailov. Ďalšie súvisia s chybami v kontrole oprávnení a autentifikácie. Viac informácií na stránke.

Zraniteľnosť snapd v Ubuntu umožňuje získať oprávnenia root

Vývojári Ubuntu opravili vysoko závažnú zraniteľnosť v komponente snap-confine aplikácie snapd, ktorá umožňuje lokálnemu útočníkovi s nízkymi oprávneniami získať oprávnenia používateľa root. Viac informácií na stránke.

WP2shell: zraniteľnosti jadra WordPress umožňujú vykonávať kód

V jadre redakčného systému WordPress boli opravené dve zraniteľnosti, ktoré po zreťazení umožňujú vzdialene vykonávať kód bez potreby autentifikácie. Existuje pre ne verejne dostupný exploit. Zraniteľnosti dostali spoločný názov wp2shell. Viac informácií na stránke.