MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

JÚN 2026

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci jún 21 kritických a 97 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritická zraniteľnosť CVE-2026-33828 **Windows Device Health Attestation (DHA)** vyplýva z porušenia hranice medzi dôveryhodnými a nedôveryhodnými dátami. Lokálny útočník s nízkymi oprávneniami ju môže zneužiť na **zvýšenie svojich oprávnení** až na úroveň SYSTEM.

Sedem kritických zraniteľností sa nachádza v komponente **Windows Remote Desktop Client**. CVE-2026-42985, CVE-2026-44801, CVE-2026-47654 a CVE-2026-48563 súvisia s možnosťou opätovného využitia deakolovanej pamäte. CVE-2026-42992, CVE-2026-44799 a CVE-2026-47289 vyplývajú z pretečenia vyrovnávacej pamäte na halde. Zraniteľnosti môže zneužiť neautorizovaný útočník na **vzdialené vykonanie kódu**. Stačí, keď sa obeť pripojí zraniteľným klinetom na jeho Remote Desktop Server.

Kritická zraniteľnosť CVE-2026-42987 v komponente **Windows Deployment Services (WDS)** súvisí s možnosťou použitia dealokovaného miesta v pamäti. Neautorizovaný útočník ju môže zneužiť na **vzdialené vykonanie kódu**. Na to potrebuje poslať špeciálne vytvorenú požiadavku zraniteľnému serveru Windows s povolenou rolou Windows Deployment Services (WDS) a vyhrať súbeh procesov.

Kritické zraniteľnosti CVE-2026-44803 a CVE-2026-44812 vo **Windows Graphics Component Win32K- GRFX** súvisia s pretečením celočíselnej premennej. Lokálny útočník bez oprávnení ju môže zneužiť na **vykonanie ľubovoľného kódu**. Útočník potrebuje presvedčiť obeť, aby otvorila špeciálne vytvorený súbor, alebo zobrazila náhľad (Preview Pane) v Prieskumníkovi (File Explorer).

Kritická zraniteľnosť CVE-2026-44810 v **Microsoft Cryptographic Services** vyplýva z nevhodného procesu autentifikácie. Lokálny neautorizovaný útočník ju môže zneužiť na **zvýšenie svojich oprávnení** až na úroveň SYSTEM. Útočník na to môže presvedčiť obeť, aby otvorila špeciálne vytvorený súbor, alebo sa môže prihlásiť do systému a spustiť špeciálne vytvorenú aplikáciu.

Kritická zraniteľnosť CVE-2026-44815 v službe **Windows DHCP Client** súvisí s pretečením vyrovnávacej pamäte zásobníka. Neautorizovaný útočník ju môže zneužiť na **vzdialené vykonanie kódu**. Na to môže použiť DHCP server pod svojou kontrolou, na ktorý pošle požiadavku DHCP klient obete.

Kritické zraniteľnosti CVE-2026-45607, CVE-2026-45641 a CVE-2026-47652 vo **Windows Hyper-V** súvisia s možnosťou čítania pamäte mimo povolené hodnoty, zámenou typu premennej a s pretečením vyrovnávacej pamäte na halde. Lokálny útočník môže prvé dve zneužiť bez oprávnení na **vykonanie ľubovoľného kódu**. Pre zneužitie tretej potrebuje vysoké oprávnenia. Útočník môže zneužiť špeciálne vytrovené požiadavky na operácie so súbormi, resp. požiadavku so špeciálne vytvoreným veľkým obsahom v rámci hosťovského virtuálneho systému na získanie prístupu do hostiteľského operačného systému.

Kritická zraniteľnosť CVE-2026-45648 vo **Windows Active Directory Domain Services** súvisí s pretečením vyrovnávacej pamäte zásobníka. Autorizovaný útočník s nízkymi oprávneniami ju môže zneužiť na **vzdialené vykonanie kódu**. Na to potrebuje prístup k rozhraniu NSPI RPC, cez ktoré odošle špeciálne vytvorený vstup vedúci k zápisu do pamäte mimo povolené hodnoty.

Kritická zraniteľnosť CVE-2026-45657 vo **Windows Kernel** súvisí so spôsobom, akým jadro spracúva dáta TCP/IP. Chyba vedie ku možnosti opätovného použitia dealokovanej pamäte. Neautorizovaný útočník ju môže zneužiť na **vzdialené vykonanie kódu** s oprávneniami SYSTEM. Na to potrebuje zraniteľnému systému poslať špeciálne vytvorené sieťové požiadavky.

Kritická zraniteľnosť CVE-2026-47288 vo **Windows Kerberos KDC** súvisí s pretečením celočíselnej premennej. Autorizovaný útočník s nízkymi oprávneniami na rovnakom segmente siete ako obeť ju môže zneužiť na **vzdialené vykonanie kódu**. Na to potrebuje odoslať špeciálne vytvorené autentifikačné požiadavky doménovému kontroléru.

Kritická zraniteľnosť CVE-2026-47291 v komponente **HTTP.sys** súvisí s pretečením celočíselnej premennej. Neautorizovaný útočník ju môže zneužiť na **vzdialené vykonanie kódu**. Na to potrebuje odoslať špeciálne vytvorený HTTP paket, ktorý spracuje http.sys na zraniteľnom systéme.

Kritická zraniteľnosť CVE-2026-48574 komponentu **Windows Media** súvisí s pretečením vyrovnávacej pamäte na halde. Lokálny neautorizovaný útočník ju môže zneužiť na **vykonanie ľubovoľného kódu**. Na to potrebuje interakciu obete.

Vysoko závažné zraniteľnosti CVE-2026-42909, CVE-2026-42913, CVE-2026-42974, CVE-2026-42981, CVE-2026-42993, CVE-2026-45599, CVE-2026-45635, CVE-2026-45636 a CVE-2026-47653 sa nachádzajú v komponentoch **Remote Desktop Client**, **Windows Performance Monitor**, **Windows UPnP Device Host** a **Windows NTFS**. Vzdialený útočník by ich mohol zneužiť na **vzdialené vykonanie kódu** a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Ostatné zraniteľnosti vysokej závažnosti možno zneužiť na eskaláciu privilégií, zneprístupnenie služby (DoS), získanie prístupu k citlivým informáciám, spoofingové útoky a odchádzanie bezpečnostných prvkov.

ZRANITEĽNÉ SYSTÉMY:

- Remote Desktop client for Windows Desktop
- 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 Client for Windows Desktop
- Windows Narrator Braille
- 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)

- Windows Server, version 2004 (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-2026-33828
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42985
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42987
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42992
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44799
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44801
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44803
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44810
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44812
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44815
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45607
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45641
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45648
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45657
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47288
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47289
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47291
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47652
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47654
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-48563
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-48574

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 jún bezpečnostné aktualizácie, ktoré opravujú 15 kritických a 49 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritické zraniteľnosti CVE-2026-44803 a CVE-2026-44812 vo **Windows Graphics Component Win32K- GRFX** súvisia s pretečením celočíselnej premennej. Lokálny útočník bez oprávnení ju môže zneužiť na **vykonanie ľubovoľného kódu**. Útočník potrebuje presvedčiť obeť, aby otvorila špeciálne vytvorený súbor, alebo zobrazila náhľad (Preview Pane) v Prieskumníkovi (File Explorer).

V **Microsoft Outlook** a **Word** boli opravené tri kritické zraniteľnosti, ktoré môže neautorizovaný útočník zneužiť na **lokálne vykonanie ľubovoľného kódu**. CVE-2026-45456 vyplýva zo zámeny typu premennej, CVE-2026-45458 súvisí s možnosťou opätovného použitia dealokovaného miesta v pamäti a CVE-2026-47635 je spôsobená pretečením vyrovnávacej pamäte na halde. Útočným vektorom pre zneužitie zraniteľností môže byť aj náhľad dokumentu (Preview Pane).

Kritické zraniteľnosti CVE-2026-45461, CVE-2026-45472 a CVE-2026-45474 balíkov **Microsoft Office** vyplývajú z možnosti opätovného použitia dealokovaného miesta v pamäti. Neautorizovaný útočník ich môže zneužiť na **lokálne vykonanie ľubovoľného kódu**. Útočným vektorom pre zneužitie zraniteľností môže byť aj náhľad dokumentu (Preview Pane).

Microsoft Office obsahuje tiež kritickú zraniteľnosť CVE-2026-45460, ktorá umožňuje lokálnemu neautorizovanému útočníkovi **získať prístup ku citlivým informáciám** uložené v pamäti haldy. Súvisí s možnosťou čítania pamäte mimo povolené hodnoty. Pre jej zneužitie musí presvedčiť obeť, aby otvorila špeciálne pripravený súbor MS Office. Útočným vektorom pre zneužitie zraniteľnosti môže byť aj náhľad dokumentu (Preview Pane).

Kritická zraniteľnosť CVE-2026-45463 balíkov **Microsoft Office** umožňuje neautorizovanému útočníkovi **lokálne vykonávať ľubovoľný kód**. Spôsobuje ju pretečenie vyrovnávacej pamäte na halde a podtečenie celočíselnej premennej. Útočným vektorom pre zneužitie tejto zraniteľnosti môže byť aj náhľad dokumentu (Preview Pane).

Štyri kritické zraniteľnosti **M365 Copilot** opravila spoločnosť Microsoft na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre ich odstránenie. Zraniteľnosti s označením CVE-2026-42824 a CVE-2026-54130 môže neautorizovaný vzdialený útočník zneužiť na **získanie prístupu k citlivým informáciám**. Chyby zabezpečenia súvisia s nevhodným ošetrením špeciálnych znakov, čo umožňuje injektovať príkazy a s absentujúcou autentifikáciou. Chyba zabezpečenia CVE-2026-45497 súvisí s nevhodným ošetrením špeciálnych znakov, čo umožňuje útočníkom s nízkymi oprávneniami **vzdialene vykonávať kód**. Posledná zraniteľnosť CVE-2026-47645 v komponente Business Chat umožňuje vzdialenému neautorizovanému útočníkovi vykonať presmerovanie na nedôveryhodnú stránku a **zvýšiť svoje oprávnenia**.

Kritická zraniteľnosť **Microsoft Copilot** s označením CVE-2026-42895 súvisí s nevhodným ošetrením špeciálnych znakov, čo umožňuje injektovať príkazy. Chybu zabezpečenia môže vzdialený útočník s nízkymi oprávneniami zneužiť na **zasahovanie do systému**. Zraniteľnosť opravila spoločnosť Microsoft na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre jej odstránenie.

Vysoko závažné zraniteľnosti spočívajú v deserializácii nedôveryhodných dát, použití dealokovaného miesta v pamäti, nevhodnej kontrole prístupov, dereferencii nedôveryhodných ukazovateľov, pretečení vyrovnávacej pamäte na halde, možnosti čítania pamäte mimo povolené hodnoty, zámene typu premennej, vzniku súbehu, prístupnosti súborov externým entitám a nedostatočnom alebo absentujúcom ošetrení používateľských vstupov. Predmetné

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

ZRANITEĽNÉ SYSTÉMY:

- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft 365 Copilot
- Microsoft Bing Search for Android
- Microsoft Excel 2016 (32-bit edition)
- Microsoft Excel 2016 (64-bit edition)
- Microsoft Excel for Android
- 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 for Android
- Microsoft PowerToys
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription Edition
- Microsoft Teams for Android
- Microsoft Word 2016 (32-bit edition)

- Microsoft Word 2016 (64-bit edition)
- Microsoft Word for Android
- Office Online Server

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-2026-42824
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42895
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44803
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-44812
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45456
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45458
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45460
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45461
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45463
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45472
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45474
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45497
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47635
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47645
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-54130

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 jún opravila jednu kritickú a jednu vysoko závažnú zraniteľnosť vo webovom prehliadači Microsoft Edge.

Kritická zraniteľnosť komponentu Microsoft Entra ID s identifikátorom CVE-2026-32208 spočíva v nevhodnej sanitizácii nedôveryhodných vstupov pri generovaní webstránok a umožňuje vzdialenému útočníkovi s nízkymi oprávneniami vykonávať spoofingové útoky typu XSS. Zraniteľnosť opravila spoločnosť Microsoft na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre jej odstránenie.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2026-50521 spočíva v možnosti opätovného použitia dealokovaného miesta v pamäti a umožňuje útočníkovi s nízkymi oprávneniami vzdialene vykonávať kód. Zneužitie zraniteľnosti môže viesť aj k úniku prihlasovacích údajov obete.

Zraniteľné systémy:

- Microsoft Edge (Chromium-based) verzie staršie ako 149.0.4022.68

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-2026-32208
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50521

MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci jún opravila 21 vysoko závažných zraniteľností v líniách internetových prehliadačov Firefox, Firefox ESR a Firefox iOS.

Línia Firefox obsahuje chybu zabezpečenia CVE-2026-10701, ktorá súvisí s nesprávne nastavenými hraničnými podmienkami. Nachádza sa v komponente Graphics: Text.

Vysoko závažná zraniteľnosť CVE-2026-10702 sa nachádza v komponente JavaScript Engine: JIT a súvisí s chybným procesom kompilácie. Zasahuje líniu Firefox.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť CVE-2026-12289, ktorá umožňuje **eskaláciu oprávnení**. Chyba zabezpečenia sa nachádza v komponente Graphics: WebRender.

Zraniteľnosť CVE-2026-12291 v líniách Firefox a Firefox ESR umožňuje **použitie dealokovaného miesta v pamäti**. Nachádza sa v komponente Networking: HTTP.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť CVE-2026-12292, ktorá súvisí s nesprávne nastavenými hraničnými podmienkami. Chyba zabezpečenia sa nachádza v komponente Web Audio.

Línia Firefox obsahuje chybu zabezpečenia, ktorá umožňuje **použitie dealokovaného miesta v pamäti**. Zraniteľnosť CVE-2026-12293 sa nachádza v komponente Graphics: WebGPU.

Spoločnosť Mozilla opravila štyri vysoko závažné zraniteľnosti v líniách prehliadačov Firefox a Firefox ESR, ktoré umožňujú **uniknúť zo sandboxu**. CVE-2026-12294 sa nachádza v komponente DOM: Workers, CVE-2026-12295 v DOM: Navigation a CVE-2026-12296 v Security: Process Sandboxing. Zraniteľnosť CVE-2026-12297 komponentu Networking vyplýva z nesprávne nastavených hraničných podmienok.

Vysoko závažná zraniteľnosť CVE-2026-12299 sa nachádza v komponente DOM: Core & HTML a súvisí s chybným procesom kompilácie. Zasahuje línie Firefox a Firefox ESR.

Firefox for iOS obsahuje v čitateľskom móde dve vysoko závažné zraniteľnosti, ktoré umožňujú **vykonávať kód JavaScript**. Chyba zabezpečenia CVE-2026-9308 súvisí s nevhodným poradím nahradzovania obsahu v HTML šablóne, čo umožňuje útočníkovi získať priestor pre vloženie obsahu JSON-LD. Zraniteľnosť CVE-2026-9309 súvisí s nevhodným spôsobom ošetrenia HTML tagov v metadátach JSON-LD, čo môže viesť k úniku a zneužitiu citlivých URL parametrov.

Zraniteľnosti CVE-2026-53899 a CVE-2026-53900 v línii Firefox for iOS súvisia s narábaním so súbormi cookies pri pristupovaní k odkazom v PDF. Prvá zraniteľnosť môže viesť k **úniku informácií v cookies**, druhá umožňuje **injektovať cookies** do požiadaviek pre nesúvisiacu cieľovú doménu.

Identifikátory CVE-2026-12326 a CVE-2026-14241 v línii Firefox, CVE-2026-12329 vo Firefox ESR a identifikátory CVE-2026-12328, CVE-2026-12290 a CVE-2026-12298 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 152.0.4
- Mozilla Firefox ESR verzie staršej ako 115.37 a 140.12
- Firefox for iOS verzie staršej ako 152.0

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 152.0.4, Firefox ESR na verziu 115.37 alebo 140.12 a Firefox for iOS aspoň na verziu 152.0.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-53/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-54/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-56/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-57/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-58/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-59/

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-62/

GOOGLE CHROME

V mesiaci jún spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 75 kritických a 295 vysoko závažných zraniteľností.

V komponente **Accessibility** bola opravená kritická zraniteľnosť CVE-2026-12009, ktorá vyplýva z nedostatočnej kontroly nedôveryhodných vstupov.

Komponent **ANGLE** obsahuje 5 kritických zraniteľností. Chyby zabezpečenia CVE-2026-10881, CVE-2026-10883 a CVE-2026-10889 umožňujú čítať pamäť a zapisovať do pamäte mimo povolené hodnoty. Chyba CVE-2026-13780 súvisí s nedostatočnou kontrolou nedôveryhodných vstupov. CVE-2026-14398 umožňuje opätovné použitie dealokovanej pamäte.

Kritická chyba zabezpečenia CVE-2026-11631 sa nachádza v komponente **Aura** a umožňuje opätovne použiť dealokovanú pamäť.

Dve kritické zraniteľnosti CVE-2026-11636 a CVE-2026-13038 v komponente **Autofill** umožňujú opätovné použitie dealokovanej pamäte.

V komponente **Blink** bola opravená kritická zraniteľnosť CVE-2026-13033, ktorá umožňuje čítať pamäť mimo povolené hodnoty.

Kritické zraniteľnosti CVE-2026-11633, CVE-2026-11635, CVE-2026-11641 a CVE-2026-13785 v komponente **Bluetooth** umožňujú opätovné použitie dealokovanej pamäte.

Kritická zraniteľnosť CVE-2026-13782 v komponente **Browser**, CVE-2026-10888 v **Cast Streaming**, CVE-2026-10890 v **Cast**, CVE-2026-11639 v **Composing** a CVE-2026-12007 v **Core** umožňuje opätovné použitie dealokovanej pamäte.

Komponent **Dawn** obsahuje tri kritické zraniteľnosti. CVE-2026-13776 súvisí so zámenou typu premennej, CVE-2026-14417 dovoľuje opätovné použitie dealokovanej pamäte a CVE-2026-14420 dovoľuje čítanie a zápis do pamäte mimo povolené hodnoty.

Kritické zraniteľnosti CVE-2026-12008, CVE-2026-12439 a CVE-2026-12440 sa nachádzajú v komponente **Digital Credentials**. Umožňujú opätovné použitie dealokovanej pamäte. Rovnaký druh zraniteľností obsahuje komponent **Extensions** (CVE-2026-13774), **File Input** (CVE-2026-11630 a CVE-2026-12441), **FileSystem** (CVE-2026-10886), **Fullscreen** (CVE-2026-13788), **Gamepad** (CVE-2026-11634) a **GFX** (CVE-2026-10891).

Komponent **GPU** obsahuje päť kritických zraniteľností. CVE-2026-10892 a CVE-2026-10897 umožňujú zapisovať do pamäte mimo povolené hodnoty. CVE-2026-10898 a CVE-2026-12010

súvisia s pretečením vyrovnávacej pamäte na zásobníku a na halde. CVE-2026-13775 dovoľuje opätovné použitie dealokovanej pamäte.

Kritické zraniteľnosti CVE-2026-10887, CVE-2026-10893, CVE-2026-13779 a CVE-2026-13787 v komponente **Chromoting** umožňujú opätovné použitie dealokovanej pamäte. Rovnaký druh zraniteľností obsahuje komponent **Chromecast** (CVE-2026-10884), a tiež **Chrome for iOS** (CVE-2026-10885, CVE-2026-10896).

V komponente **iOSWeb** bola objavené kritická zraniteľnosť CVE-2026-13777, ktorá vyplýva z nedostatočnej validácie nedôveryhodných vstupov.

Kritická zraniteľnosť CVE-2026-11640 v komponente **libyuv** spočíva v pretečení celočíselnej premennej.

Vo viacerých komponentoch Google Chrome boli opravené kritické zraniteľnosti umožňujúce opätovné použitie dealokovanej pamäte. V komponente **Network** bola opravená CVE-2026-10882, v **Proxy** CVE-2026-11643 a v **Printing** CVE-2026-10894 a CVE-2026-11638. V **Passwords** boli opravené CVE-2026-10900, CVE-2026-10901 a CVE-2026-12442. V komponente **Ozone** boli opravené CVE-2026-10895, CVE-2026-10899, CVE-2026-10902, CVE-2026-11628, CVE-2026-11629 a CVE-2026-13786.

Komponent **Skia** obsahuje tri kritické zraniteľnosti. Chyba zabezpečenia CVE-2026-13781 vyplýva z nedostatočnej validácie nedôveryhodných vstupov, CVE-2026-14419 umožňuje opätovné použitie dealokovanej pamäte a CVE-2026-14427 súvisí s pretečením vyrovnávacej pamäte na halde.

Ďalšie kritické chyby zabezpečenia umožňujúce opätovné použitie dealokovanej pamäte boli opravené v komponentoch **TabStrip** (CVE-2026-11632), **Views** (CVE-2026-11637, CVE-2026-11644, CVE-2026-13783 a CVE-2026-13784), **Web Apps** (CVE-2026-11642) a **WebAuthentication** (CVE-2026-12443).

Kritické zraniteľnosti CVE-2026-13028 a CVE-2026-13032 v komponente **WebGL** umožňujú opätovne použiť dealokovanú pamäť.

Opätovne použiť dealokovanú pamäť umožňuje aj kritická zraniteľnosť CVE-2026-12011 v komponente **WebMIDI**, CVE-2026-12437 vo **WebShare** a CVE-2026-13778 vo **WebUSB**.

Komponent **WebView** obsahuje kritickú zraniteľnosť CVE-2026-12438. Súvisí s nevhodnou implementáciou nešpecifikovaného prvku.

Spoločnosť Google opravila vysoko závažné zraniteľnosti v komponentoch **Accessibility, Actor, AdFilter, ANGLE, Audio, Autofill, Bindings, Blink, Bluetooth, Browser, CameraCapture, Canvas, Cast, Codecs, Core, CSS, Dawn, DeviceBoundSessionCredentials, DevTools, Digital Credentials API, DOM, Downloads, Enterprise, Extensions, File Input, File System Access, FileSystem, Forms, Fullscreen, GFX, Glic, GPU, Guest View, Headless, Chrome for iOS, Chrome Tabs, Chromecast,**

Chromoting, IME, Import, Input, InterestGroups, Journeys, libyuv, Linux Toolkit Theming, Media, MediaCapture, Metrics, MimeHandlerView, Mojo, Navigation, Network, New Tab Page, Ozone, Passwords, Payments, PDF, Plugins, Printing, QUIC, Read Anything, Safe Browsing, Scroll, Serial, ServiceWorker, Settings, Skia, SurfaceCapture, SVG, TabStrip, Tint, Touchbar, UI, Updater, USB, V8, Video, VideoCapture, Views, ViewTransitions, Viz, WebAppInstalls, WebAuthentication, WebCodecs, WebRTC, WebShare, WebView, WebXR a XML. Tieto dovoľujú čítať a zapisovať do pamäte mimo povolené hodnoty, použiť dealokovanú pamäť a neinicializované zdroje, súvisia s pretečenia medzipamäte na halde 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, nesprávnej implementácie bezpečnosti UI a umožňujú injektovať skripty a získavať informácie bočnými kanálmi.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows verzie staršej ako 150.0.7871.46/.47
- Google Chrome pre Mac verzie staršej ako 150.0.7871.46/.47
- Google Chrome pre Linux verzie staršej ako 150.0.7871.46

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows aspoň na verziu 150.0.7871.46/.47, Mac aspoň na verziu 150.0.7871.46/.47 a Linux aspoň na verziu 150.0.7871.46.

ZDROJE:

- https://chromereleases.googleblog.com/2026/06
- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html
- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_01962725236.html
- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_01750511403.html

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0482630350.html
- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_01245939337.html
- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0175352312.html

4. ADOBE ACROBAT A READER

V mesiaci jún spoločnosť Adobe opravila 16 vysoko závažných zraniteľností v produktoch Adobe Acrobat a Reader.

Zraniteľnosti CVE-2026-47911 a CVE-2026-47965 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-2026-47912, CVE-2026-47913, CVE-2026-47914, CVE-2026-47915, CVE-2026-47916, CVE-2026-47917, CVE-2026-47918, CVE-2026-47919, CVE-2026-47920, CVE-2026-47921 a CVE-2026-47955 môže lokálny útočník bez autorizácie zneužiť na **vykonanie ľubovoľného kódu.**

Vysoko závažná zraniteľnosť CVE-2026-47959 súvisí s pretečením vyrovnávacej pamäte zásobníka. Lokálny útočník bez autorizácie ju môže zneužiť na **vykonanie ľubovoľného kódu**.

Vysoko závažná zraniteľnosť CVE-2026-47952 súvisí s pretečením vyrovnávacej pamäte haldy. Lokálny útočník bez autorizácie ju môže zneužiť na **vykonanie ľubovoľného kódu**.

Posledná opravená vysoko závažná zraniteľnosť vzniká kvôli absentujúcej kontrole elementu vyhľadávacej cesty. CVE-2026-47937 môže lokálny útočník s vysokými oprávneniami zneužiť na **vykonanie ľubovoľného kódu**.

ZRANITEĽNÉ SYSTÉMY:

- Acrobat a Acrobat Reader pre Windows a Mac verzie 26.001.21651 a staršie
- Acrobat 2024 pre Windows a Mac verzie 24.001.30365 a staršie

ODPORÚČANIA:

Odporúčame aktualizáciu aspoň na verziu:

- Acrobat a Acrobat Reader pre Windows a Mac 26.001.21662
- Acrobat 2024 pre Windows a Mac 24.001.30383

ZDROJE:

- https://helpx.adobe.com/security/security-bulletin.html#acrobat
- https://helpx.adobe.com/security/products/acrobat/apsb26-63.html

5. FRAMEWORKY

MICROSOFT .NET FRAMEWORK

V mesiaci jún spoločnosť Microsoft opravila 3 vysoko závažné zraniteľnosti vo frameworku .NET.

Vysoko závažná zraniteľnosť CVE-2026-45490 v .NET Core SDK spočíva v nevhodnom spôsobe autorizácie. Lokálnemu útočníkovi s nízkymi oprávneniami umožňuje **navýšiť svoje oprávnenia** až na úroveň SYSTEM.

Vysoko závažná zraniteľnosť CVE-2026-45491 v .NET súvisí s nevhodným spôsobom narábania s odkazmi pred prístupom ku súborom. Neautorizovanému lokálnemu útočníkovi umožňuje vykonávať neoprávnené **zásahy do systému**.

Chyba zabezpečenia .NET, ASP.NET a Microsoft Visual Studio s označením CVE-2026-45591 súvisí s absentujúcim obmedzením využívania výpočtových zdrojov. Vzdialený neautentifikovaný útočník ju môže zneužiť na spôsobenie **nedostupnosti 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
- .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 8.0
- ASP.NET Core 9.0

ODPORÚČANIA:

Odporúčame aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávača.

ZDROJE:

- https://msrc.microsoft.com/update-guide/en-us
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45490
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45491
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45591

ORACLE JAVA

Spoločnosť Oracle plánuje vydať veľkú sadu opráv 21. júla 2026.

ZDROJE:

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

INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

ZRANITEĽNOSŤ PALO ALTO NETWORKS PAN-OS UMOŽŇUJE OBÍSŤ PRIHLASOVANIE

Spoločnosť Palo Alto Networks opravila aktívne zneužívanú zraniteľnosť v riešení GlobalProtect v PAN-OS a Prisma Access, ktorá umožňuje neautentifikovaným vzdialeným útočníkom podvrhovať súbory cookies pre prihlásenie prostredníctvom funkcie „Authentication Override“ a vytvárať tak neautorizované spojenia VPN. Viac informácií na stránke.

SAP OPRAVIL V JÚNI KRITICKÉ ZRANITEĽNOSTI V NETWEAVERI A COMMERCE CLOUD

Spoločnosť SAP vydala bezpečnostné aktualizácie systémov SAP NetWeaver a SAP Commerce Cloud, ktoré opravujú 15 zraniteľností, z čoho 4 sú označené ako kritické. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ VEEAM BACKUP & REPLICATION

Spoločnosť Veeam vydala bezpečnostné aktualizácie na svoj produkt Backup & Replication, ktorá opravuje kritickú zraniteľnosť. CVE-2026-44963 umožňuje doménovému používateľovi vzdialené vykonanie kódu na zálohovacom serveri. Viac informácií na stránke.

ZREŤAZENÉ ZRANITEĽNOSTI V UNIFI OS UMOŽŇUJÚ PREVZATIE KONTROLY NAD SERVEROM

Spoločnosť Ubiquiti opravila kritické zraniteľnosti viacerých zariadení v platforme UniFi OS. Zreťazenie troch z nich umožňuje vzdialenému neautentifikovanému útočníkovi získať v systéme reverzný shell s oprávneniami používateľa root prostredníctvom jedinej špeciálne vytvorenej HTTP požiadavky. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ KRITICKÁ ZRANITEĽNOSŤ CHECK POINT REMOTE ACCESS VPN, MOBILE ACCESS SSL/VPN A SPARK FIREWALL

Spoločnosť Check Point opravila aktívne zneužívanú kritickú zraniteľnosť produktov Remote Access VPN, Mobile Access SSL/VPN a Spark Firewall, ktorá umožňuje obísť autentifikáciu a

vytvárať VPN relácie. Chyba zabezpečenia vyplýva z logickej chyby pri validácii certifikátov v rámci protokolu IKEv1. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V PRODUKTE IVANTI SENTRY

Spoločnosť Ivanti vydala bezpečnostné aktualizácie na svoj produkt Ivanti Sentry, ktoré opravujú dve kritické zraniteľnosti. Zraniteľnosti umožňujú získanie administrátorských oprávnení a schopnosti vykonávať vzdialene kód. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ SPLUNK ENTERPRISE UMOŽŇUJE VZDIALENE VYKONÁVAŤ KÓD

Spoločnosť Splunk vydala bezpečnostné aktualizácie pre kritickú zraniteľnosť v Splunk Enterprise, ktorá umožňuje neautentifikovaným útočníkom manipulovať s databázou PostgreSQL, vykonávať operácie so súbormi a zneužitím viacerých koncových bodov dosiahnuť vzdialené vykonanie kódu. Viac informácií na stránke.

ZRANITEĽNOSTI V PROTOBUFJS OHROZUJÚ DÁTOVÉ A AI SYSTÉMY

Výskumníci zo spoločnosti Cyera objavili šesť zraniteľností v knižnici protobufjs, ktorá patrí medzi najpoužívanejšie JavaScript implementácie formátu Protocol Buffers a tvorí základ komunikácie v cloudových službách, databázach, AI platformách a distribuovaných aplikáciách. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ ZRANITEĽNOSŤ CISCO CATALYST SD-WAN MANAGER

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu produktu Catalyst SD-WAN Manager, ktorá opravuje aktívne zneužívanú zraniteľnosť CVE-2026-20262 vo webovom používateľskom rozhraní. Chyba zabezpečenia umožňuje autentifikovanému útočníkovi vytvárať a prepisovať súbory v systéme a následne získať oprávnenia používateľa root. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI NGINX UMOŽŇUJÚ ZNEFUNKČNIŤ SLUŽBU A VYKONÁVAŤ KÓD

Spoločnosť F5 vydala bezpečnostné aktualizácie na opravu dvoch kritických zraniteľností v produktoch NGINX, ktoré môžu v niektorých konfiguráciách umožniť vzdialenému útočníkovi vyvolať zlyhanie služby (DoS) alebo spustiť škodlivý kód. Viac informácií na stránke.