MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

MÁJ 2026

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci máj 6 kritických a 61 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritická zraniteľnosť CVE-2026-32161 v ovládači **Windows Native WiFi Miniport Driver** súvisí s možnosťou použitia dealokovaného miesta v pamäti. Neautorizovaný útočník na rovnakom segmente siete ako obeť ju môže zneužiť na **vzdialené vykonanie kódu**. Na to potrebuje vyhrať súbeh procesov.

Kritická zraniteľnosť CVE-2026-35421 komponentu **Windows GDI** súvisí s pretečením vyrovnávacej pamäte na halde. Lokálny neautorizovaný útočník ju môže zneužiť na **vykonanie ľubovoľného kódu**. Na to potrebuje presvedčiť obeť, aby otvorila špeciálne vytvorený súbor typu Enhanced Metafile (EMF) v aplikácii Microsoft Paint.

Kritická zraniteľnosť CVE-2026-40402 **Windows Hyper-V** vyplýva z možnosti opätovného použitia dealokovanej pamäte. Lokálny neautorizovaný útočník ju môže zneužiť na **zvýšenie svojich oprávnení** až na úroveň SYSTEM. Útočník môže zneužiť hosťovský virtuálny systém s nízkymi oprávneniami na získanie prístupu do hostiteľského systému.

Kritická zraniteľnosť CVE-2026-40403 **Windows Graphics Component Win32K - GRFX** súvisí s pretečením vyrovnávacej pamäte na halde. Lokálny útočník s nízkymi oprávneniami ju môže zneužiť na **vykonanie ľubovoľného kódu**. Útočník môže zneužiť hosťovský virtuálny systém na získanie prístupu do hostiteľského operačného systému.

Kritická zraniteľnosť CVE-2026-41089 **Windows Netlogon** súvisí s pretečením vyrovnávacej pamäte na zásobníku. Vzdialený neautorizovaný útočník ju môže zneužiť na **vykonanie ľubovoľného kódu**. Útočník ju môže zneužiť zaslaním špeciálne vytvorenej sieťovej požiadavky doménovému kontroléru.

Kritická zraniteľnosť CVE-2026-41096 v komponente **Windows DNS Client** súvisí s pretečením vyrovnávacej pamäte na halde. Vzdialený neautorizovaný útočník ju môže zneužiť na **vzdialené vykonanie kódu** zaslaním špeciálne vytvorenej DNS odpovede zraniteľnému systému.

Vysoko závažné zraniteľnosti CVE-2026-34329, CVE-2026-34332, CVE-2026-40380 a CVE-2026-40415 sa nachádzajú v komponentoch **Microsoft Message Queuing (MSMQ)**, **Windows Kernel-Mode Driver**, **Windows Volume Manager Extension Driver** a **Windows TCP/IP**. 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 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 Admin Center
- 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 2022, 23H2 Edition (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-2026-32161
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35421
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40402
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40403
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41089
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41096

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 máj bezpečnostné aktualizácie, ktoré opravujú 14 kritických a 23 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Microsoft Office obsahuje tri kritické bezpečnostné zraniteľnosti, ktoré umožňujú lokálnemu neautorizovanému útočníkovi vykonávať ľubovoľný kód. Zraniteľnosť s označením CVE-2026-40358 umožňuje opätovné použitie dealokovaného miesta v pamäti, CVE-2026-40363 a CVE-2026-42831 súvisia s pretečením medzipamäte na halde. V prípade prvých dvoch môže byť útočným vektorom aj náhľad dokumentu (Preview Pane). Posledná zraniteľnosť vyžaduje interakciu obete, ktorá musí otvoriť škodlivý súbor MS Office.

Kritickú zraniteľnosť Microsoft SharePoint s označením CVE-2026-40365 môže prihlásený útočník s nízkymi oprávneniami zneužiť na vzdialené vykonanie ľubovoľného kódu na zraniteľnej inštancii SharePoint Server. Chyba zabezpečenia vyplýva z neošetrenej deserializácie nedôveryhodných údajov. Útočným vektorom môže byť aj náhľad dokumentu (Preview Pane).

Microsoft Word obsahuje tri kritické zraniteľnosti, ktoré môže neautorizovaný útočník zneužiť na lokálne vykonanie ľubovoľného kódu. Chyba zabezpečenia s označením CVE-2026-40364 súvisí s pretečením medzipamäte na halde a vyplýva zo zámeny typu premennej a použitia neinicializovaných zdrojov. CVE-2026-40366 vyplýva z možnosti opätovného použitia dealokovaného miesta v pamäti. CVE-2026-40367 súvisí s neošetrenou dereferenciou nedôveryhodného ukazovateľa v pamäti. Útočným vektorom pre zneužitie zraniteľností môže byť aj náhľad dokumentu (Preview Pane).

Kritická zraniteľnosť CVE-2026-40361 v Microsoft Word a Outlook súvisí s možnosťou opätovného použitia dealokovaného miesta v pamäti. Neautorizovaný útočník ju môže zneužiť na lokálne vykonanie ľubovoľného kódu. Útočným vektorom pre zneužitie zraniteľností môže byť aj náhľad dokumentu (Preview Pane).

Microsoft Authenticator obsahuje kritickú zraniteľnosť CVE-2026-41615, ktorú môže vzdialený neautorizovaný útočník zneužiť na **získanie prístupu k citlivým informáciám**, konkrétne ku prihlasovacím tokenom obete. To mu následne umožní pristupovať ku interným informáciám organizácie.

Tri kritické zraniteľnosti **M365 Copilot** opravila spoločnosť Microsoft na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre ich odstránenie. Zraniteľnosti s označením CVE-2026-26129, CVE-2026-26164 a CVE-2026-42827 môže neautorizovaný vzdialený útočník zneužiť na **získanie prístupu k citlivým informáciám**. Chyby zabezpečenia súvisia s nevhodným ošetrením špeciálnych znakov, čo umožňuje injektovať príkazy.

Kritická zraniteľnosť **Microsoft Copilot** s označením CVE-2026-41090 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.

Aj v **Microsoft Teams** opravila spoločnosť Microsoft kritickú zraniteľnosť na svojich systémoch. Nie je potrebné vykonať ďalšie aktivity pre jej odstránenie. Zraniteľnosť s označením CVE-2026-33823 vyplýva z nevhodného spôsobu prideľovania oprávnení. Vzdialený útočník s nízkymi oprávneniami ju môže zneužiť na **získanie prístupu k citlivým informáciám**.

Vysoko závažné zraniteľnosti spočívajú v deserializácii nedôveryhodných dát, použití dealokovaného miesta v pamäti, nevhodnej kontrole prístupov, pretečení vyrovnávacej pamäte na halde, možnosti čítania pamäte mimo povolené hodnoty, 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** a **útoky typu spoofing**.

ZRANITEĽNÉ SYSTÉMY:

- M365 Copilot for Desktop
- 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 Android
- Microsoft 365 Copilot for iOS
- Microsoft 365 Copilot's Business Chat
- Microsoft Authenticator for Android
- Microsoft Authenticator for IOS

- 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 for Android
- Microsoft Office LTSC 2021 for 32-bit editions
- Microsoft Office LTSC 2021 for 64-bit editions
- Microsoft Office LTSC 2024 for 32-bit editions
- Microsoft Office LTSC 2024 for 64-bit editions
- Microsoft Office LTSC for Mac 2021
- Microsoft Office LTSC for Mac 2024
- Microsoft Outlook for iOS
- Microsoft PowerPoint for Android
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription Edition
- Microsoft Teams
- 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-2026-26129
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26164
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33823
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40358
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40361
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40363
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40364
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40365
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40366
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40367
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41090
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41615
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42827
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42831

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 máj opravila dve vysoko závažné zraniteľnosti vo webovom prehliadači Microsoft Edge.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2026-42838 spočíva v nevhodnej sanitizácii špeciálnych znakov a umožňuje vzdialenému neautorizovanému útočníkovi **navýšiť svoje privilégiá** na úroveň aktuálneho používateľa. Zneužitie zraniteľnosti vyžaduje interakciu zo strany obete.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2026-45495 spočíva v neošetrenej možnosti prechádzania adresármi a umožňuje neautorizovanému útočníkovi **vzdialene vykonávať kód**. Zneužitie zraniteľnosti vyžaduje interakciu zo strany obete.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft Edge (Chromium-based) verzie staršie ako 148.0.3967.70

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-2026-42838
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45495

MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci máj opravila 17 vysoko závažných zraniteľností v línii internetových prehliadačov Firefox, Firefox ESR a Firefox iOS.

Línie Firefox a Firefox ESR obsahujú chybu zabezpečenia, ktorá umožňuje **použitie dealokovaného miesta v pamäti**. Zraniteľnosť CVE-2026-8090 sa nachádza v komponente DOM: Networking.

Línia Firefox ESR obsahuje zraniteľnosť CVE-2026-8091, ktorá súvisí s nesprávne nastavenými hraničnými podmienkami. Chyba zabezpečenia sa nachádza v komponente Audio/Video: Playback.

Vysoko závažná zraniteľnosť nešpecifikovaného druhu CVE-2026-8094 sa nachádza v komponente WebRTC v línii Firefox ESR.

Vysoko závažné zraniteľnosti CVE-2026-8388 a CVE-2026-8389 sa nachádzajú v komponente JavaScript Engine: JIT a súvisia s chybným procesom kompilácie. Prvá zasahuje línie Firefox a Firefox ESR, druhá líniu Firefox.

Línia Firefox obsahuje chybu zabezpečenia, ktorá umožňuje **použitie dealokovaného miesta v pamäti**. Zraniteľnosť CVE-2026-8390 sa nachádza v komponente JavaScript: WebAssembly.

Vysoko závažná zraniteľnosť nešpecifikovaného druhu CVE-2026-8391 sa nachádza v komponente JavaScript Engine v líniách Firefox a Firefox ESR.

Zraniteľnosť komponentu Profile Backup CVE-2026-8401 v líniách Firefox a Firefox ESR umožňuje **uniknúť zo sandboxu**. Rovnako to umožňuje chyba zabezpečenia CVE-2026-8945 v líniách Firefox a Firefox for Android.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť CVE-2026-8946, ktorá súvisí s nesprávne nastavenými hraničnými podmienkami. Chyba zabezpečenia sa nachádza v komponente Audio/Video: Web Codecs.

Zraniteľnosť CVE-2026-8947 v líniách Firefox a Firefox ESR umožňuje **použitie dealokovaného miesta v pamäti**. Nachádza sa v komponente DOM: Bindings (WebIDL).

Zraniteľnosť CVE-2026-8948 v línii Firefox umožňuje **obchádzať politiku Same-origin**. Nachádza sa v komponente DOM: Networking.

Firefox for iOS obsahuje v čitateľskom móde vysoko závažnú zraniteľnosť CVE-2026-8706, ktorá môže viesť k **úniku citlivých používateľských informácií**.

Identifikátory CVE-2026-8093 a CVE-2026-8973 v línii Firefox a indikátory CVE-2026-8092 a CVE-2026-8975 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 151
- Mozilla Firefox ESR verzie staršej ako 115.36 a 140.11
- Firefox for iOS verzie staršej ako 151.0

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 151, Firefox ESR na verziu 115.36 alebo 140.11 a Firefox for iOS aspoň na verziu 151.0.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-40/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-41/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-42/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-45/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-46/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-47/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-48/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-49/

GOOGLE CHROME

V mesiaci máj spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 41 kritických a 199 vysoko závažných zraniteľností.

Komponent ANGLE obsahuje 5 kritických zraniteľností. Chyby zabezpečenia CVE-2026-8519 a CVE-2026-9882 vyplývajú z pretečenia celočíselnej premennej. Chyby CVE-2026-9877 a CVE-2026-9878 umožňujú opätovné použitie dealokovanej pamäte. CVE-2026-9879 umožňuje zapisovať do pamäte mimo povolené hodnoty.

Kritická chyba zabezpečenia CVE-2026-8514 sa nachádza v komponente Aura a umožňuje opätovne použiť dealokovanú pamäť.

Dve kritické zraniteľnosti CVE-2026-9883 a CVE-2026-9886 v komponente **Base** umožňujú opätovné použitie dealokovanej pamäte.

V komponente **Blink** boli opravené dve kritické zraniteľnosti. CVE-2026-7896 vyplýva z pretečenia celočíselnej premennej a CVE-2026-8518 umožňuje opätovné použitie dealokovanej pamäte.

Kritická zraniteľnosť CVE-2026-9881 v komponente **Bluetooth** umožňuje opätovné použitie dealokovanej pamäte.

Kritická zraniteľnosť CVE-2026-9884 sa nachádza v komponente **Browser**. Umožňuje opätovné použitie dealokovanej pamäte.

Kritická zraniteľnosť CVE-2026-8516 sa nachádza v komponente **DataTransfer**. Vyplýva z nedostatočného overovania nedôveryhodných vstupov.

Komponent **Dawn** obsahuje dve kritické. CVE-2026-9874 dovoľuje opätovné použitie dealokovanej pamäte a CVE-2026-9889 dovoľuje čítanie a zápis do pamäte mimo povolené hodnoty.

Kritická zraniteľnosť CVE-2026-8522 sa nachádza v komponente **Downloads**. Umožňuje opätovné použitie dealokovanej pamäte.

Podobné zraniteľnosti sa nachádzajú v komponentoch **Extensions**, **FileSystem**, **HID**, **Mobile**, **Chromoting**, **Input** a **Network**. CVE-2026-9891, CVE-2026-8512, CVE-2026-8515, CVE-2026-7897, CVE-2026-7898, CVE-2026-8513 a CVE-2026-9873 umožňujú opätovné použitie dealokovanej pamäte.

Komponent **GPU** obsahuje kritickú zraniteľnosť CVE-2026-9872, ktorá umožňuje zapisovať do pamäte mimo povolené hodnoty.

Kritická zraniteľnosť CVE-2026-8520 v komponente **Payments** vyplýva zo vzniku súbehu procesov.

Kritická zraniteľnosť CVE-2026-9887 sa nachádza v komponente **Proxy**. Umožňuje opätovné použitie dealokovanej pamäte.

Komponent **Skia** obsahuje tri kritické zraniteľnosti. Chyba zabezpečenia CVE-2026-8510 vyplýva z pretečenia celočíselnej premennej, CVE-2026-9892 súvisí s nevhodnou implementáciou nešpecifikovaných prvkov a CVE-2026-9893 umožňuje zapisovať do pamäte mimo povolené hodnoty.

Kritická zraniteľnosť CVE-2026-8521 sa nachádza v komponente **Tab Groups**. Umožňuje opätovné použitie dealokovanej pamäte.

Komponent UI obsahuje tri kritické zraniteľnosti. Chyba zabezpečenia CVE-2026-8511 umožňuje zapisovať do pamäte mimo povolené hodnoty. CVE-2026-9111 súvisí s nevhodnou implementáciou nešpecifikovaných prvkov a CVE-2026-9885 vyplýva z nedostatočnej validácie nedôveryhodných dát.

Kritické zraniteľnosti CVE-2026-9875 a CVE-2026-9876 v komponente WebGL umožňujú čítať pamäť mimo povolené hodnoty a opätovne použiť dealokovanú pamäť. CVE-2026-9880 vyplýva z nedostatočnej validácie nedôveryhodných vstupov.

Komponenty WebRTC, WebView a XR obsahujú kritické zraniteľnosti CVE-2026-9110, CVE-2026-9888 a CVE-2026-9890. Tieto dovoľujú opätovné použitie dealokovanej pamäte.

Komponent WebML obsahuje kritickú zraniteľnosť CVE-2026-8509. Súvisí s pretečením vyrovnávacej pamäte na halde.

Kritická zraniteľnosť WebShare vyplýva z nešpecifikovanej chyby v rámci životného cyklu objektu.

Spoločnosť Google opravila vysoko závažné zraniteľnosti v komponentoch Accessibility, ANGLE, Aura, Bluetooth, Codecs, Compositing, Core, Dawn, DevTools, DOM, Downloads, FileSystem, Fonts, Fullscreen, Gamepad, GFX, Glic, Google Lens, GPU, GTK, Chromoting, Input, InterestGroups, Internationalization, iOS, Media, MediaRecording, Mojo, Network, OptimizationGuide, Passwords, PDF, PDFium, PerformanceManager, PresentationAPI, Printing, QUIC, ReadingMode, Runtime, SanitizerAPI, ServiceWorker, Site Isolation, Skia, SurfaceCapture, SVG, TabStrip, Tint, UI, USB, V8, Views, ViewTransitions, WebAppInstalls, WebAudio, WebCodecs, WebGL, WebMIDI, WebML, WebRTC, WebShare, WebXR, WTF, XML a XR. 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 nedôveryhodných vstupov. Spôsobujú poškodenie objektov a umožňujú injektovať skripty.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows verzie staršej ako 148.0.7778.216/217
- Google Chrome pre Mac verzie staršej ako 148.0.7778.215/216
- Google Chrome pre Linux verzie staršej ako 148.0.7778.215

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows aspoň na verziu 148.0.7778.216/217, Mac aspoň na verziu 148.0.7778.215/216 a Linux aspoň na verziu 148.0.7778.215.

ZDROJE:

- https://chromereleases.googleblog.com/2026/05
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0841193308.html
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html

4. ADOBE ACROBAT A READER

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

Zraniteľnosti CVE-2026-34621 a CVE-2026-34622 súvisia s nedostatočnou kontrolou modifikácie atribútov prototypov objektov. Lokálny útočník bez autorizácie ich môže zneužiť na vykonanie ľubovoľného kódu.

ZDROJE:

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

5. FRAMEWORKY

MICROSOFT .NET FRAMEWORK

V mesiaci máj spoločnosť Microsoft opravila 4 vysoko závažné zraniteľnosti vo frameworku .NET.

Vysoko závažná zraniteľnosť CVE-2026-32175 v .NET Core a Microsoft Visual Studio spočíva v nevhodnom spôsobe narábania so špeciálne vytvorenými súbormi. Vzdialenému útočníkovi s nízkymi oprávneniami umožňuje prechádzať adresármi a **zapisovať ľubovoľné súbory a zložky** na nešpecifikované miesta systému.

Vysoko závažná zraniteľnosť CVE-2026-32177 v .NET, .NET Framework a Microsoft Visual Studio súvisí s nevhodným spôsobom validácie vstupov a s pretečením vyrovnávacej pamäte na halde. Neautorizovanému lokálnemu útočníkovi umožňuje spôsobiť **navýšiť oprávnenia**. Tak môže získať **prístup ku prihlasovacím údajom používateľov**, **upravovať súbory na serveri** a **spôsobiť nedostupnosť systému**. Pre úspešné zneužitie zraniteľnosti útočník potrebuje, aby obeť spustila škodlivý obsah v aplikácii.

Vysoko závažná zraniteľnosť CVE-2026-35433 v .NET a .NET Framework súvisí s nevhodným spôsobom validácie vstupov a s pretečením celočíselnej premennej. Neautorizovanému lokálnemu útočníkovi umožňuje spôsobiť **navýšiť oprávnenia na úroveň SYSTEM**. Pre úspešné zneužitie zraniteľnosti útočník potrebuje, aby obeť spustila škodlivý obsah v aplikácii.

Chyba zabezpečenia .NET s označením CVE-2026-42899 súvisí so vznikom nekonečnej slučky v ASP.NET Core. 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 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

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-2026-32175
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32177
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35433
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42899

ORACLE JAVA

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

ZDROJE:

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

INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

COPY FAIL: AKTÍVNE ZNEUŽÍVANÁ ZRANITEĽNOSŤ LINUXOVÉHO JADRA

Jadro operačných systémov Linux obsahuje od roku 2017 vysoko závažnú zraniteľnosť, ktorá umožňuje neprivilegovanému používateľovi zapisovať do pamäte v rámci page cache súborov. Môže tak prepisovať bajty, ktoré definujú jeho oprávnenia, čím môže získať oprávnenia používateľa root. Zraniteľnosť je aktívne zneužívaná. Viac informácií na stránke.

ZRANITEĽNOSTI V PROGRESS MOVEIT AUTOMATION UMOŽŇUJÚ ZÍSKANIE ADMINISTRÁTORSKÉHO PRÍSTUPU

Spoločnosť Progress Software vydala bezpečnostné aktualizácie nástroja pre spravovaný prenos súborov (MFT), MOVEit Automation, ktoré opravujú jednu kritickú a jednu vysoko závažnú zraniteľnosť. Zraniteľnosti sa nachádzajú v backendových príkazových rozhraniach a umožňujú obídenie autentifikácie a eskaláciu privilégií. Viac informácií na stránke.

ZRANITEĽNOSŤ V APACHE HTTP SERVER UMOŽŇUJE ZNEPRÍSTUPNENIE SLUŽBY A VZDIALENÉ VYKONANIE KÓDU

Spoločnosť Cisco opravila vysoko závažnú zraniteľnosť zariadení Crosswork Network Controller (CNC) a Network Services Orchestrator (NSO), ktorá umožňuje vyčerpať kapacitu sieťových spojení a vyvolať nedostupnosť služby na zraniteľnom zariadení. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI VM2 UMOŽŇUJÚ UNIKAŤ ZO SANDBOXU

Vývojári knižnice vm2 pre Node.js opravili sady kritických zraniteľností, ktoré umožňujú vzdialeným neautorizovaným útočníkom uniknúť zo sandboxu a vykonávať kód v hostiteľskom prostredí. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ KRITICKÁ ZRANITEĽNOSŤ PALO ALTO NETWORKS PAN-OS UMOŽŇUJE VYKONÁVAŤ KÓD AKO ROOT

Spoločnosť Palo Alto Networks opravila kritickú aktívne zneužívanú zraniteľnosť v PAN-OS firewallov sérií PA a VM, nakonfigurovaných ako User-ID Authentication Portal. Vzdialený útočník ju môže zneužiť na vykonanie škodlivého kódu s oprávneniami používateľa root. Viac informácií na stránke.

NGINX Rift: 18 rokov stará zraniteľnosť umožňuje DoS a vzdialené vykonávanie kódu

Vývojári webového servera NGINX opravili 18 rokov starú zraniteľnosť NGINX Rift, ktorá umožňuje vzdialenému neautentifikovanému útočníkovi zaslaním HTTP požiadavky spôsobiť nedostupnosť servera, a tiež mu umožňuje vykonávať kód. Zraniteľnosť je aktívne zneužívaná. Viac informácií na stránke.

Kritické zraniteľnosti vo Fortinet FortiAuthenticator a FortiSandbox umožňujú vzdialené vykonanie kódu

Spoločnosť Fortinet vydala bezpečnostné aktualizácie, ktoré opravujú dve kritické zraniteľnosti v platformách FortiSandbox a FortiAuthenticator umožňujúce spúšťať príkazy alebo ľubovoľný kód na neopravených systémoch. Viac informácií na stránke.

Kritická zraniteľnosť mailových serverov Exim umožňuje poškodenie obsahu pamäte

Spoločnosť Exim vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť v mail serveroch Exim, ktoré využívajú knižnicu GnuTLS. Jej zneužitie môže spôsobiť poškodenie pamäte a umožniť vzdialené vykonanie kódu. Viac informácií na stránke.

SAP opravila viaceré kritické a vysoko závažné zraniteľnosti

Spoločnosť SAP vydala sadu opráv zraniteľností vo viacerých svojich produktoch. Dve z nich sú klasifikované ako kritické a jedna ako vysoko závažná. Umožňujú vzdialene vykonávať kód a príkazy operačného systému, získať prístup k citlivým údajom, alebo spôsobiť nedostupnosť aplikácie. Viac informácií na stránke.

Kritická zraniteľnosť Drupal umožňuje injektovať príkazy SQL

Vývojári platformy Drupal vydali opravné aktualizácie pre zraniteľnosť, ktorú označili ako vysoko kritickú. Táto chyba zabezpečenia umožňuje neautorizovaným vzdialeným útočníkom zasielať špeciálne vytvorené požiadavky, ktoré zneužívajú nevhodnú sanitizáciu a umožňujú injektovať príkazy SQL. Viac informácií na stránke.

HP Linux Imaging and Printing Software má dve závažné zraniteľnosti

Vývojári spoločnosti HP opravili jednu kritickú a jednu vysoko závažnú zraniteľnosť v aplikácii HP Linux Imaging and Printing Software. Chyby zabezpečenia umožňujú eskalovať oprávnenia a vykonávať príkazy na hostiteľskom operačnom systéme. Viac informácií na stránke.

Stará zraniteľnosť jadra Linux umožňuje prevziať kontrolu nad systémom

Tím TRU spoločnosti Qualys objavil v jadre OS Linux vysoko závažnú zraniteľnosť, ktorá umožňuje lokálnemu útočníkovi bez oprávnení získať oprávnenia používateľa root, exfiltrovať prihlasovacie údaje a kľúče a vykonávať ľubovoľné príkazy. Zraniteľnosť bola do jadra zavedená ešte v roku 2016. Viac informácií na stránke.

Cisco Secure Workload má kritickú zraniteľnosť v REST API

Spoločnosť Cisco opravila kritickú zraniteľnosť v produkte Secure Workload, ktorá dovoľuje vzdialeným neautentifikovaným útočníkom prostredníctvom rozhrania REST API získať oprávnenia Site Admin. Útočníci môžu pristupovať k citlivým informáciám a meniť konfiguračné nastavenia. Viac informácií na stránke.

Kritické zraniteľnosti Ubiquiti UniFi OS

Ubiquiti vydala bezpečnostné aktualizácie pre UniFi OS, ktoré opravujú tri kritické zraniteľnosti CVE-2026-34908, CVE-2026-34909 a CVE-2026-34910. Tieto umožňujú vzdialeným útočníkom bez oprávnení vykonávať neautorizované zmeny v systéme, získať prístup k súborom alebo vykonávať príkazy. Zraniteľnosti ovplyvňujú široké spektrum zariadení vrátane UDM Pro, UDR, UNVR či UniFi OS Server. Viac informácií na stránke.

Zraniteľnosť Gitea umožňuje voľne pristupovať k privátnym kontajnerom

Vysoko závažná zraniteľnosť v open-source platforme Gitea umožňuje neautentifikovaným vzdialeným útočníkom získať prístup k súkromným kontajnerom a obsahu privátnych projektov bez platných oprávnení alebo vytvoreného účtu na platforme. Viac informácií na stránke.