MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

MAREC 2026

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci marec 47 vysoko závažných zraniteľností v operačných systémoch Windows.

Vysoko závažné zraniteľnosti CVE-2026-23669, CVE-2026-24288, CVE-2026-25172, CVE-2026-25173, CVE-2026-25190 a CVE-2026-26111 sa nachádzajú v komponentoch Windows Routing and Remote Access Service (RRAS), GDI Windows Mobile Broadband Driver aRPC Runtime Library. 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, odchádzanie bezpečnostných prvkov a spoofingové útoky.

Zraniteľné systémy:

- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 11 Version 23H2 for ARM64-based Systems
- Windows 11 Version 23H2 for x64-based Systems
- Windows 11 Version 24H2 for ARM64-based Systems
- Windows 11 Version 24H2 for x64-based Systems

- Windows 11 Version 25H2 for ARM64-based Systems
- Windows 11 Version 25H2 for x64-based Systems
- Windows 11 Version 26H1 for ARM64-based Systems
- Windows 11 version 26H1 for x64-based Systems
- Windows App Client for Windows Desktop
- 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

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 októbra 2026. Podmienkou môže byť prihlásenie sa cez Microsoft account.

Pre Windows 11 Microsoft plánovane ukončí podporu pre v súčasnosti podporované verzie nasledovne:

23H2 Home a Pro: Podpora **skončila** 11. decembra 2025.
23H2 Enterprise a Education: Podpora skončí 10. decembra 2026.

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. 25H2.

2. KANCELÁRSKE BALÍKY MICROSOFT OFFICE A OFFICE WEB APPS

Spoločnosť Microsoft vydala v mesiaci marec bezpečnostné aktualizácie, ktoré opravujú 7 kritických a 12 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritickú zraniteľnosť **M365 Copilot** s označením CVE-2026-24299 môže neautorizovaný vzdialený útočník zneužiť na **získanie citlivých informácií**. Chyba zabezpečenia súvisí s nevhodnou sanitizáciou špeciálnych znakov používaných v príkazoch. Spoločnosť Microsoft zraniteľnosť opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre jej odstránenie.

Kritickú zraniteľnosť **Microsoft Office** s označením CVE-2026-26110 môže neautorizovaný útočník zneužiť na **lokálne vykonanie ľubovoľného kódu**. Chyba zabezpečenia vyplýva zo zámeny typu premennej. Útočným vektorom môže byť aj náhľad dokumentu (Preview Pane).

Kritická zraniteľnosť **Microsoft Office** s označením CVE-2026-26113 súvisí s dereferenciou nedôveryhodného ukazovateľa. Neautorizovaný útočník zneužiť na **lokálne vykonanie ľubovoľného kódu**. Útočným vektorom môže byť aj náhľad dokumentu (Preview Pane).

Kritickú zraniteľnosť **Microsoft Bing** s označením CVE-2026-26120 môže vzdialený útočník zneužiť pri **neautorizovaných zásahoch na serveri**. Chyba zabezpečenia umožňuje vykonávať

útoky typu SSRF. Spoločnosť Microsoft zraniteľnosť opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre jej odstránenie.

Kritické zraniteľnosti **Microsoft Purview** s označením CVE-2026-26138 a CVE-2026-26139 môže vzdialený neautorizovaný útočník zneužiť na **eskaláciu oprávnení**. Chyba zabezpečenia umožňuje vykonávať útoky typu SSRF. Spoločnosť Microsoft zraniteľnosť opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre jej odstránenie.

Kritickú zraniteľnosť **Microsoft Excel** s označením CVE-2026-26144 môže neautorizovaný vzdialený útočník zneužiť na sieťovú **exfiltráciu citlivých dát** cez mód Copilot Agent. Chyba zabezpečenia súvisí s nevhodnou sanitizáciou používateľských vstupov počas generovania webstránky a dovoľuje vykonávať útoky typu XSS.

Vysoko závažné zraniteľnosti spočívajú v pretečení vyrovnávacej pamäte na halde, použití dealokovaného miesta v pamäti, pretečení celočíselnej premennej, deserializácii nedôveryhodných dát, dereferencii nedôveryhodného ukazovateľa, možnosti čítania pamäte mimo povolené hodnoty, neošetrení používateľských vstupov a nevhodnej autorizácii. Predmetné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu, eskaláciu oprávnení, získavanie citlivých informácií** 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 365 Copilot for Android
- Microsoft 365 Copilot for iOS
- Microsoft Authenticator for Android
- Microsoft Authenticator for IOS
- Microsoft Bing
- Microsoft Excel 2016 (32-bit edition)
- Microsoft Excel 2016 (64-bit edition)
- Microsoft Excel for Android
- Microsoft Excel for iOS
- Microsoft Loop for iOS
- 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 OneNote for Android
- Microsoft OneNote for iOS
- Microsoft Outlook for Android
- Microsoft Outlook for iOS
- Microsoft Outlook for Mac
- Microsoft PowerPoint for Android
- Microsoft PowerPoint for iOS
- Microsoft Purview
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription Edition
- Microsoft Teams for Android
- Microsoft Teams for iOS
- Microsoft Word for Android
- Microsoft Word for iOS
- 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-2026-24299
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26110
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26113
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26120
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26138
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26139
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26144

Koniec podpory pre Office 2016 a Office 2019

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.

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 marec opravila jednu vysoko závažnú zraniteľnosť vo webovom prehliadači Microsoft Edge pre iOS a Android.

Zraniteľnosť CVE-2026-26133 súvisí s možnosťou injektovania príkazov do M365 Copilot, čo môže vzdialený neautorizovaný útočník zneužiť pre získavanie citlivých informácií. Útočník môže pomocou škodlivého e-mailu dosiahnuť, aby Copilot zobrazil obeti legitímne pôsobiaci phishingový e-mail s odkazom na škodlivú webstránku.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft Edge pre iOS a Android, verzie staršie ako 145.3800.99

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
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26133

MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci marec opravila 23 vysoko závažných zraniteľností v línii internetových prehliadačov Firefox a Firefox ESR.

Zraniteľnosť CVE-2026-3845 sa nachádza v línii Firefox pre Android súvisí s pretečením zásobníka na halde v komponente Audio/Video: Playback.

Zraniteľnosť CVE-2026-3846 v komponente CSS Parsing and Computation línie Firefox vyplýva z možnosti obídenia politiky same-origin.

Zraniteľnosť CVE-2026-4684 v komponente Graphics: WebRender v líniách Firefox a Firefox ESR súvisí so súbehom procesov a umožňuje použitie dealokovaného miesta v pamäti.

Viacero opravených zraniteľností v líniách Firefox a Firefox ESR súvisí s nesprávne nastavenými hraničnými podmienkami. Chyby s identifikátormi CVE-2026-4685 a CVE-2026-4686 sa nachádzajú v komponente Graphics: Canvas2D, CVE-2026-4693 v komponente Audio/Video: Playback a CVE-2026-4694 v komponente Graphics. Zraniteľnosti CVE-2026-4695 a CVE-2026-4697 sa nachádzajú v komponente Audio/Video: Web Codecs a chyba zabezpečenia CVE-2026-4699 v komponente Layout: Text and Fonts. Zraniteľnosť CVE-2026-4709 sa nachádza v komponente Audio/Video: GMP. Zraniteľnosť CVE-2026-4687 sa nachádza v komponente Telemetry a umožňuje únik zo sandboxu.

Chyby zabezpečenia línií Firefox a Firefox ESR CVE-2026-4689 a CVE-2026-4690 v komponente XPCOM súvisia s nesprávne nastavenými hraničnými podmienkami a pretečením celočíselnej premennej. Umožňujú únik zo sandboxu.

Únik zo sandboxu v líniách Firefox a Firefox ESR umožňuje vysoko závažná zraniteľnosť CVE-2026-4688 v komponente Disability Access APIs kvôli možnosti **použitia dealokovaného miesta v pamäti**, a tiež CVE-2026-4692 v Responsive Design Mode.

Línie Firefox a Firofex ESR obsahujú tiež dve zraniteľnosti, ktoré umožňujú **použitie dealokovaného miesta v pamäti**. Zraniteľnosť CVE-2026-4691 sa nachádza v komponente CSS Parsing and Computation, a CVE-2026-4696 v komponente Layout: Text and Fonts.

Zraniteľnosť CVE-2026-4698 v líniách Firefox a Firefox ESR sa nachádza v komponente JavaScript Engine: JIT. Vyplýva z chybnej kompilácie v nástroji JIT.

Identifikátory CVE-2026-3847 a CVE-2026-4729 v línii Firefox a indikátory CVE-2026-4720 a CVE-2026-4721 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 staršie ako 149
- Mozilla Firefox ESR verzie staršej ako 115.34 a 140.9

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 149 a Firefox ESR na verziu 115.34 alebo 140.9.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-19/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-20/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-21/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-22/

GOOGLE CHROME

V mesiaci marec spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 7 kritických a 69 vysoko závažných zraniteľností.

Vysoko závažná zraniteľnosť CVE-2026-3917 v komponente **Agents** umožňuje opätovné použitie dealokovanej pamäte.

Komponent **ANGLE** obsahuje jednu kritickú a 5 vysoko závažných zraniteľností. Kritická chyba zabezpečenia CVE-2026-3536 vyplýva z pretečenia celočíselnej premennej. Vysoko závažné CVE-2026-4448 a CVE-2026-5275 súvisia s pretečením vyrovnávacej pamäte na halde. CVE-2026-4452 a CVE-2026-5277 súvisia s pretečením celočíselnej premennej. CVE-2026-5283 vyplýva z nevhodnej implementácie nešpecifikovaných prvkov.

Kritická zraniteľnosť CVE-2026-4441 sa nachádza v komponente **Base**. Umožňuje opätovné použitie dealokovanej pamäte.

V komponente **Blink** boli opravené dve vysoko závažné zraniteľnosti. CVE-2026-4449 umožňuje opätovné použitie dealokovanej pamäte a CVE-2026-4462 dovoľuje čítať obsah pamäte mimo povolené hodnoty.

Vysoko závažná chyba zabezpečenia CVE-2026-5274 sa nachádza v komponente **Codecs** a súvisí s pretečením celočíselnej premennej.

Kritická zraniteľnosť CVE-2026-5290 sa nachádza v komponente **Compositing**. Umožňuje opätovné použitie dealokovanej pamäte.

Komponent **CSS** obsahuje 4 vysoko závažné zraniteľnosti. CVE-2026-3541 vyplýva z nevhodnej implementácie nešpecifikovaných prvkov, CVE-2026-4442 súvisí s pretečením vyrovnávacej pamäte na halde, CVE-2026-4674 dovoľuje čítať obsah pamäte mimo povolené hodnoty a CVE-2026-5273 umožňuje opätovné použitie dealokovanej pamäte.

Komponent **Dawn** obsahuje 5 vysoko závažných zraniteľností. CVE-2026-4453 súvisí s pretečením celočíselnej premennej, zatiaľ čo CVE-2026-4676, CVE-2026-5281, CVE-2026-5284 a CVE-2026-5286 dovoľujú opätovné použitie dealokovanej pamäte. Zraniteľnosť CVE-2026-5281 je **aktívne zneužívaná**.

Vysoko závažná zraniteľnosť CVE-2026-3539 v komponente **DevTools** vyplýva z nešpecifikovaných problémov spojených so životným cyklom objektu.

Vysoko závažná zraniteľnosť CVE-2026-4456 sa nachádza v komponente **Digital Credentials API**. Umožňuje opätovné použitie dealokovanej pamäte.

Komponent **Extensions** obsahuje dve vysoko závažné zraniteľnosti. CVE-2026-3919 a CVE-2026-4458 umožňuje opätovné použitie dealokovanej pamäte.

Vysoko závažná zraniteľnosť CVE-2026-4680 v komponente **FedCM** umožňuje opätovné použitie dealokovanej pamäte.

Vysoko závažná zraniteľnosť CVE-2026-4679 v komponente **Fonts** súvisí s pretečením celočíselnej premennej.

Komponent **GPU** obsahuje vysoko závažnú zraniteľnosť CVE-2026-5272, ktorá súvisí s pretečením vyrovnávacej pamäte na halde.

Vysoko závažná zraniteľnosť CVE-2026-3922 v komponente **MediaStream** umožňuje opätovné použitie dealokovanej pamäte.

Komponent **Navigation** obsahuje 3 vysoko závažné zraniteľnosti. CVE-2026-3545 vyplýva z nedostatočnej validácie nešpecifikovaných dát, CVE-2026-4451 súvisí s nedostatočnou validáciou nedôveryhodných vstupov a CVE-2026-5289 dovoľuje opätovné použitie dealokovanej pamäte.

Vysoko závažná zraniteľnosť CVE-2026-4454 v komponente **Network** umožňuje opätovné použitie dealokovanej pamäte.

Vysoko závažná zraniteľnosť CVE-2026-5287 v komponente **PDF** umožňuje opätovné použitie dealokovanej pamäte.

Vysoko závažná zraniteľnosť CVE-2026-4455 v komponente **PDFium** súvisí s pretečením vyrovnávacej pamäte na halde.

Kritickú zraniteľnosť obsahuje komponent **PowerVR**. CVE-2026-3537 vyplýva z nešpecifikovaných problémov spojených so životným cyklom objektu.

Komponent **Skia** obsahuje jednu kritickú a dve vysoko závažné zraniteľnosti. Kritická chyba zabezpečenia CVE-2026-3538 vyplýva z pretečenia celočíselnej premennej. Vysoko závažné CVE-2026-3909 dovoľuje zapisovať do pamäte mimo povolené hodnoty a CVE-2026-4460 umožňuje čítať obsah pamäte mimo povolené hodnoty. Zraniteľnosť CVE-2026-3909 je **aktívne zneužívaná**.

Vysoko závažná zraniteľnosť CVE-2026-3921 v komponente **TextEncoding** umožňuje opätovné použitie dealokovanej pamäte.

Komponent **V8** obsahuje 7 vysoko závažných zraniteľností. CVE-2026-3543, CVE-2026-3910, CVE-2026-4447 a CVE-2026-4461 vyplývajú z nevhodnej implementácie nešpecifikovaných prvkov. CVE-2026-4450 umožňuje zapisovať do pamäte mimo povolené hodnoty. CVE-2026-4457 vyplýva zo zámeny typu premennej. CVE-2026-5279 vedie ku poškodeniu nešpecifikovaného objektu. Zraniteľnosť CVE-2026-3910 je **aktívne zneužívaná**.

Vysoko závažná zraniteľnosť CVE-2026-3916 v komponente **Web Speech** umožňuje čítať obsah pamäte mimo povolené hodnoty.

Komponent **WebAssembly** obsahuje vysoko závažnú zraniteľnosť CVE-2026-3542, ktorá vyplýva z nevhodnej implementácie nešpecifikovaných prvkov.

Komponent **WebAudio** obsahuje 5 vysoko závažných zraniteľností. CVE-2026-3540 vyplýva z nevhodnej implementácie nešpecifikovaných prvkov. CVE-2026-4450 a CVE-2026-4673 súvisia s pretečením vyrovnávacej pamäte na halde. CVE-2026-4459 umožňuje čítať a zapisovať do pamäte mimo povolené hodnoty. CVE-2026-4677 dovoľuje čítať obsah pamäte mimo povolené hodnoty.

Tri vysoko závažné zraniteľnosti boli opravené v komponente **WebCodecs**. CVE-2026-3544 súvisí s pretečením vyrovnávacej pamäte na halde. CVE-2026-5280 umožňuje opätovné použitie dealokovanej pamäte. CVE-2026-5282 dovoľuje čítať obsah pamäte mimo povolené hodnoty.

Komponent **WebGL** obsahuje dve kritické a dve vysoko závažné zraniteľnosti. Kritické CVE-2026-4439 a CVE-2026-4440 umožňujú pristupovať k pamäti mimo povolené hodnoty a vykonávať čítanie a zápis. Vysoko závažná CVE-2026-4675 súvisí s pretečením vyrovnávacej pamäte na halde a CVE-2026-5285 dovoľuje opätovné použitie dealokovanej pamäte.

Komponent **WebGPU** obsahuje vysoko závažnú zraniteľnosť CVE-2026-4678, ktorá umožňuje opätovné použitie dealokovanej pamäte.

Vysoko závažná zraniteľnosť CVE-2026-3918 v komponente **WebMCP** umožňuje opätovné použitie dealokovanej pamäte.

Dve vysoko závažné zraniteľnosti CVE-2026-3923 a CVE-2026-5278 v komponente **WebMIDI** dovoľujú opätovné použitie dealokovanej pamäte.

Komponent **WebML** obsahuje jednu kritickú a tri vysoko závažné zraniteľnosti. Kritická CVE-2026-3913 súvisí s pretečením vyrovnávacej pamäte na halde. Vysoko závažná CVE-2026-3914 súvisí s pretečením celočíselnej premennej, CVE-2026-3915 s pretečením vyrovnávacej pamäte na halde a CVE-2026-3920 umožňuje pristupovať k pamäti mimo povolené hodnoty.

Komponent **WebRTC** obsahuje 4 vysoko závažné zraniteľnosti. CVE-2026-4444 súvisí s pretečením vyrovnávacej pamäte na zásobníku a CVE-2026-4463 s pretečením na halde. CVE-2026-4445 a CVE-2026-4446 umožňujú opätovné použitie dealokovanej pamäte.

Vysoko závažná zraniteľnosť CVE-2026-5276 v komponente **WebUSB** súvisí s nedostatočným presadzovaním nešpecifikovanej politiky.

Vysoko závažná zraniteľnosť CVE-2026-5288 v komponente **WebView** umožňuje opätovné použitie dealokovanej pamäte.

Vysoko závažná zraniteľnosť komponentu **WindowDialog**, CVE-2026-3924, umožňuje opätovné použitie dealokovanej pamäte.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows verzie staršej ako 146.0.7680.177/178
- Google Chrome pre Mac verzie staršej ako 146.0.7680.177/178
- Google Chrome pre Linux verzie staršej ako 146.0.7680.177

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 146.0.7680.177/178 a Linux aspoň na verziu 146.0.7680.177.

ZDROJE:

- https://chromereleases.googleblog.com/2026/03
- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html
- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html
- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_13.html
- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_18.html
- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_23.html
- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html

4. ADOBE ACROBAT A READER

V mesiaci marec spoločnosť Adobe opravila 2 vysoko závažné zraniteľnosti v produktoch Adobe Acrobat a Reader.

Zraniteľnosť CVE-2025-27220 súvisí s možnosťou opätovného použitia dealokovaného miesta v pamäti a možno ju zneužiť na **vykonanie ľubovoľného kódu**.

Zraniteľnosť CVE-2025-27278 spočíva v možnosti opätovného použitia dealokovaného miesta v pamäti. Možno ju zneužiť na **vykonanie ľubovoľného kódu**.

ZRANITEĽNÉ SYSTÉMY:

- Acrobat DC a Acrobat Reader DC pre Windows a Mac verzie 25.001.21265, a staršie
- Acrobat 2024 pre Windows verzie 24.001.30307 a Mac verzie 24.001.30308, a staršie

ODPORÚČANIA:

Odporúčame aktualizáciu aspoň na verziu:

- Acrobat DC a Acrobat Reader DC pre Windows a Mac 25.001.21288
- Acrobat 2024 pre Windows a Mac 24.001.30356

ZDROJE:

- https://helpx.adobe.com/security/security-bulletin.html#acrobat
- https://helpx.adobe.com/security/products/acrobat/apsb26-26.html

5. FRAMEWORKY

MICROSOFT .NET FRAMEWORK

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

CVE-2026-26127 v .NET spočíva v možnosti čítania pamäte mimo povolené hodnoty. Neautorizovanému vzdialenému útočníkovi umožňuje spôsobiť **nedostupnosť služby (DoS)**.

ASP.NET Core obsahuje zraniteľnosť CVE-2026-26130, ktorá spočíva v nesprávnom narábaní so zdrojmi, čo vyplýva z absentujúcich limitov a obmedzení. To umožňuje neautorizovanému vzdialenému útočníkovi spôsobiť **nedostupnosť služby (DoS)**.

Chyba zabezpečenia .NET s označením CVE-2026-26131 súvisí s nesprávnym nastavením štandardných povolení. Lokálnemu útočníkovi s nízkymi oprávneniami umožňuje **zvýšenie oprávnení** na najvyššiu úroveň.

ZRANITEĽNÉ SYSTÉMY:

- .NET 10.0 installed on Linux
- .NET 10.0 installed on Mac OS
- .NET 10.0 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
- Microsoft.Bcl.Memory 10.0
- Microsoft.Bcl.Memory 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-2026-26127
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26130
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26131

ORACLE JAVA

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

ZDROJE:

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

INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

KRITICKÁ ZRANITEĽNOSŤ CISCO CATALYST SD-WAN CONTROLLER/MANAGER

Spoločnosť Cisco opravila kritickú zraniteľnosť vo svojom produkte Catalyst SD-WAN Controller/Manager. Chybu zabezpečenia aktívne zneužívajú útočníci na obídenie autentifikácie a získanie prístupu ku konfiguračnému rozhraniu. Viac informácií na stránke.

RIEŠENIE ADVANCED ENDPOINT SECURITY OD TRENDAI OBSAHUJE KRITICKÉ ZRANITEĽNOSTI

Spoločnosť TrendAI (nové meno vetvy spoločnosti Trend Micro enterprise business) vydalo bezpečnostné aktualizácie pre svoje riešenie advanced endpoint security Apex One. Tie opravujú 8 zraniteľností z ktorých 2 sú vyhodnotené ako kritické. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ JUNOS OS EVOLVED DOVOĽUJE VYKONÁVAŤ KÓD AKO ROOT

Spoločnosť Juniper Networks opravila kritickú zraniteľnosť platformy On-Box Anomaly Detection vo svojich routeroch série PTX. Zraniteľnosť umožňuje bez autentifikácie vzdialene vykonávať kód s oprávneniami používateľa root. Viac informácií na stránke.

KEĎ Z ADMINISTRÁTORSKÝCH FUNKCIÍ VZNIKNE RCE: PRÍPADOVÁ ŠTÚDIA OTRS COMMUNITY PACKAGE DESIGN

Bezpečnostní analytici CSIRT.SK objavili chybu v dizajne tiketovacieho systému OTRS Community. Táto bezpečnostná chyba umožňuje vykonávanie ľubovoľného kódu. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V CISCO SECURE FMC A SCC UMOŽŇUJÚ VZDIALENÉ VYKONANIE KÓDU

Spoločnosť Cisco vydala bezpečnostné aktualizácie nástroja pre manažment firewallov Secure Firewall Management Center (FMC) a Security Cloud Control (SCC) Firewall Management, ktoré opravujú 2 kritické zraniteľnosti umožňujúce obídenie prihlásenia, eskaláciu oprávnení a vzdialené vykonanie kódu. Jedna zo zraniteľností bola zneužívaná ako zero-day od januára. Viac informácií na stránke.

ZÁVAŽNÉ ZRANITEĽNOSTI CISCO CATALYST SD-WAN MANAGER

Spoločnosť Cisco opravila 5 závažných zraniteľností v Catalyst SD-WAN Manager. Tieto útočníkom umožňujú manipulovať so súbormi, získavať informácie, obchádzať prihlásenie, či eskalovať svoje oprávnenia. Cisco potvrdila, že útočníci aktívne zneužívajú dve z opravených zraniteľností. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ MODULU WORDPRESS USER REGISTRATION & MEMBERSHIP

Spoločnosť WPEverest vydala bezpečnostnú aktualizáciu svojho modulu User Registration & Membership pre WordPress, ktorá opravuje aktívne zneužívanú kritickú zraniteľnosť CVE-2026-1492. Vzdialený neautentifikovaný útočník ju môže zneužiť na vytvorenie administrátorského účtu. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V HPE ARUBA NETWORKING AOS-CX UMOŽŇUJE RESET ADMINISTRÁTORSKÉHO HESLA

Spoločnosť HPE (Hewlett Packard Enterprise) vydala balík aktualizácií operačného systému prepínačov série Aruba CX, ktorý okrem iných opravuje jednu kritickú zraniteľnosť. CVE-2026-23813 umožňuje útočníkovi bez akýchkoľvek prihlasovacích údajov obísť autentifikáciu webového manažmentového rozhrania. Viac informácií na stránke.

VEEAM OPRAVUJE VIACERÉ KRITICKÉ ZRANITEĽNOSTI PRODUKTU BACKUP & REPLICATION

Spoločnosť Veeam vydala bezpečnostné aktualizácie zálohovacieho riešenia Backup & Replication, ktoré opravujú 7 zraniteľností, z čoho 5 je označených ako kritické. Vzdialenému autentifikovanému útočníkovi umožňujú vykonávanie kódu, obídenie bezpečnostných prvkov a manipuláciu so súbormi, eskaláciu privilégií a získanie prihlasovacích údajov. Viac informácií na stránke.

APPLE OPRAVILA ZRANITEĽNOSŤ KOMPONENTU WEBKIT UMOŽŇUJÚCU OBÍDENIE POLITIKY SAME ORIGIN

Spoločnosť Apple vydala bezpečnostné aktualizácie svojich operačných systémov iOS, iPadOS a macOS, ktoré opravujú zraniteľnosť komponentu WebKit. Zraniteľnosť spočíva v chybe mechanizmu CORS, ktorá vyplýva z nedostatočného overovania vstupov v rámci Navigation API. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ GNU INETUTILS TELNETD UMOŽŇUJE VZDIALENÉ VYKONANIE KÓDU

Bezpečnostní výskumníci zverejnili informácie o kritickej zraniteľnosti v GNU InetUtils telnetd. CVE-2026-32746 sa nachádza v handleri LINEMODE SLC (Set Local Characters) a umožňuje zápis do pamäte mimo povolených hodnôt. Viac informácií na stránke.

ZNEUŽÍVANÁ ZRANITEĽNOSŤ ZIMBRA COLLABORATION SUITE DOVOĽUJE PERZISTENTNÉ XSS

CISA pridala do katalógu aktívne zneužívaných zraniteľností (KEV) vysoko závažnú zraniteľnosť Zimbra Collaboration Suite. CVE-2025-66376 umožňuje neautentifikovanému útočníkovi vykonávať útoky typu XSS cez e-maily vo formáte HTML. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ SCREENCONNECT UMOŽŇUJE PRÍSTUP K RELÁCIÁM

Spoločnosť ConnectWise opravila kritickú zraniteľnosť v produkte ScreenConnect, ktorá umožňuje útočníkom získať prístup ku kryptografickému materiálu inštancie, a spolu s ním k aktívnym reláciám. Útočník môže tiež získať zvýšené oprávnenia. Spoločnosť pozorovala pokusy o zneužitie zraniteľnosti. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI CITRIX NETSCALER ADC A GATEWAY

Spoločnosť Citrix na základe interných kontrol objavila a opravila kritickú zraniteľnosť produktov Citrix NetScaler ADC a Gateway, ktorá umožňuje čítanie pamäte mimo povolené hodnoty. Zároveň opravila vysoko závažnú zraniteľnosť vedúcu ku zámene relácií používateľov. Viac informácií na stránke.

ÚTOČNÍCI ZNEUŽÍVAJÚ KRITICKÚ ZRANITEĽNOSŤ F5 BIG-IP APM

Spoločnosť F5 opravila kritickú chybu zabezpečenia na zariadeniach BIG-IP APM, ktorá môže viesť ku vykonaniu kódu na diaľku za nešpecifikovaných podmienok. Viac informácií na stránke.

ZRANITEĽNOSŤ WORDPRESS SMART SLIDER 3 UMOŽŇUJE KRÁDEŽ DÁT

Bezpečnostní výskumníci upozornili na kritickú zraniteľnosť v doplnku Smart Slider 3 pre WordPress, ktorý je aktívny na viac ako 800 000 webových stránkach. Zraniteľnosť umožňuje akémukoľvek autentifikovanému používateľovi vrátane úrovne subscriber čítať ľubovoľné súbory na serveri. Viac informácií na stránke.