MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

APRÍL 2026

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci apríl 4 kritické a 126 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritická zraniteľnosť CVE-2026-32157 v nástroji **Remote Desktop Client** súvisí s možnosťou použitia dealokovaného miesta v pamäti. Neautorizovaný útočník ju môže zneužiť na **vzdialené vykonanie kódu**. Na to potrebuje presvedčiť autorizovaného používateľa, aby cieľové zariadenie pripojil ku škodlivému serveru.

Kritická zraniteľnosť CVE-2026-33824 komponentu **Windows Internet Key Exchange (IKE) Extension** súvisí s dvojitým uvoľnením pamäte. Neautorizovaný útočník ju môže zneužiť na **vzdialené vykonanie kódu**. Na to môže poslať špeciálne upravené pakety zariadeniu s povoleným IKE v2.

Kritická zraniteľnosť CVE-2026-33826 **Windows Active Directory** vyplýva z nevhodného overovania vstupov. Autentifikovaný útočník v rovnakej doméne ju môže zneužiť na **vzdialené vykonanie kódu** s rovnakými oprávneniami, ako má služba RPC na cieľovom serveri. Na to potrebuje poslať špeciálne upravené volanie na RPC hostiteľa.

Kritická zraniteľnosť CVE-2026-33827 v komponente **TCP/IP** súvisí s využívaním zdieľaných zdrojov, resp. so vznikom súbehu. Vzdialený neautorizovaný útočník ju môže zneužiť na **vzdialené vykonanie kódu** zaslaním špeciálne upraveného paketu IPv6 uzlu s povoleným IPSec.

Vysoko závažné zraniteľnosti CVE-2026-26156, CVE-2026-32149, CVE-2026-32156, CVE-2026-32183 a CVE-2026-32221 sa nachádzajú v komponentoch **Windows Hyper-V**, **Windows UPnP**, **Windows Snipping Tool** a **Windows Graphics Component**. 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:

- 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 Admin Center
- 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
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32157
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33824
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33826
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33827

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 apríl bezpečnostné aktualizácie, ktoré opravujú 6 kritických a 11 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Microsoft Bing obsahuje dve kritické zraniteľnosti. Zraniteľnosť CVE-2026-32186 umožňuje vykonávať útoky typu SSRF, čo môže vzdialený neautorizovaný útočník zneužiť na **eskaláciu svojich oprávnení**. Zraniteľnosť CVE-2026-33819 vyplýva z neošetrenej deserializácie nedôveryhodných dát. Neautorizovaný útočník ju môže zneužiť na **vzdialené vykonanie kódu**. Spoločnosť Microsoft zraniteľnosti opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre ich odstránenie.

Kritickú zraniteľnosť **Microsoft Office** s označením CVE-2026-32190 môže neautorizovaný útočník zneužiť na **lokálne vykonanie ľubovoľného kódu**. Chyba zabezpečenia vyplýva z možnosti opätovného použitia dealokovaného miesta v pamäti. Útočným vektorom môže byť aj náhľad dokumentu (Preview Pane).

Kritickú zraniteľnosť **M365 Copilot** s označením CVE-2026-33102 môže neautorizovaný vzdialený útočník zneužiť na **eskalovanie oprávnení**. Chyba zabezpečenia súvisí s neošetreným presmerovaním na nedôveryhodné stránky (tzv. otvorené presmerovanie). Spoločnosť Microsoft zraniteľnosť opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre jej odstránenie.

Microsoft Word obsahuje dve kritické zraniteľnosti, ktoré môže neautorizovaný útočník zneužiť na **lokálne vykonanie ľubovoľného kódu**. Chyba zabezpečenia s označením CVE-2026-33114 súvisí s dereferenciou nedôveryhodného ukazovateľa v pamäti. Zraniteľnosť CVE-2026-33115 vyplýva z možnosti opätovného použitia dealokovaného miesta v pamäti. Útočným vektorom môže byť pre obe z nich aj náhľad dokumentu (Preview Pane).

Vysoko závažné zraniteľnosti spočívajú v použití dealokovaného miesta v pamäti, možnosti čítania pamäte mimo povolené hodnoty a neošetrení používateľských vstupov. Predmetné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu, 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 Bing
- Microsoft Excel 2016 (32-bit edition)
- Microsoft Excel 2016 (64-bit edition)
- Microsoft Office 2016 (32-bit edition)
- Microsoft Office 2016 (64-bit edition)
- Microsoft Office 2019 for 32-bit editions
- Microsoft Office 2019 for 64-bit editions
- Microsoft Office 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 PowerPoint 2016 (32-bit edition)
- Microsoft PowerPoint 2016 (64-bit edition)
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription Edition
- 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-2026-32186
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32190
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33102

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33114
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33115
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33819

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 apríl neopravila žiadnu kritickú alebo vysoko závažnú zraniteľnosť vo webovom prehliadači Microsoft Edge.

ZDROJE:

- https://msrc.microsoft.com/update-guide/en-us

MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci apríl opravila jednu kritickú a 20 vysoko závažných zraniteľností v línii internetových prehliadačov Firefox a Firefox ESR.

Kritická zraniteľnosť CVE-2026-7322 sa nachádza v líniách Firefox a Firefox ESR. Súvisí s chybným narábaním s pamäťou. Táto zraniteľnosť ovplyvňuje bezpečnosť pamäte a môže viesť ku poškodeniu pamäte alebo možnosti vykonávať kód.

Viacero opravených zraniteľností súvisí s nesprávne nastavenými hraničnými podmienkami. Chyba v líniách Firefox a Firefox ESR s identifikátorom CVE-2026-5732 sa nachádza v komponente Graphics: Text a zraniteľnosti CVE-2026-6752 a CVE-2026-6753 v komponente WebRTC. Chyba zabezpečenia v línii Firefox s označením CVE-2026-5733 sa nachádza v komponente Graphics: WebGPU.

Línie Firefox a Firefox ESR obsahujú tri chyby zabezpečenia, ktoré umožňujú **použitie dealokovaného miesta v pamäti**. Zraniteľnosť CVE-2026-6746 sa nachádza v komponente DOM: Core & HTML, CVE-2026-6747 v komponente WebRTC a CVE-2026-6754 v komponente JavaScript Engine.

Zraniteľnosti línií Firefox a Firefox ESR CVE-2026-6748 a CVE-2026-6751 sa nachádzajú v komponente Audio/Video: Web Codecs. Súvisia s neinicializovanou pamäťou.

Zraniteľnosť línií Firefox a Firefox ESR s označením CVE-2026-6749 v komponente Graphics: Canvas2D vyplýva z neinicializovanej pamäte a môže viesť k **úniku nešpecifikovaných informácií**.

Chyba zabezpečenia v líniách Firefox a Firefox ESR s označením CVE-2026-6750 sa nachádza v komponente Graphics: WebRender. Umožňuje **eskalovať oprávnenia** útočníka.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť CVE-2026-7320, ktorá môže viesť k **úniku nešpecifikovaných informácií**. Chyba zabezpečenia sa nachádza v komponente Audio/Video a súvisí s nesprávne nastavenými hraničnými podmienkami.

Identifikátory CVE-2026-5735, CVE-2026-6784 a CVE-2026-7324 v línii Firefox a indikátory CVE-2026-5731, CVE-2026-5734, CVE-2026-6785, CVE-2026-6786 a CVE-2026-7323 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 150.0.1
- Mozilla Firefox ESR verzie staršej ako 115.35.1 a 140.10.1

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 150.0.1 a Firefox ESR na verziu 115.35.1 alebo 140.10.1.

ZDROJE:

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

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-25/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-27/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-30/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-31/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-32/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-35/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-36/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-37/

GOOGLE CHROME

V mesiaci apríl spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 11 kritických a 61 vysoko závažných zraniteľností.

Komponent **Accessibility** obsahuje jednu kritickú a jednu vysoko závažnú zraniteľnosť. Kritická chyba zabezpečenia CVE-2026-7344 umožňuje opätovné použitie dealokovanej pamäte. Vysoko závažná CVE-2026-6311 umožňuje zneužitie neinicializovanej pamäte.

Komponent **ANGLE** obsahuje jednu kritickú a tri vysoko závažné zraniteľnosti. Kritická chyba zabezpečenia CVE-2026-6296, rovnako ako vysoko závažná CVE-2026-5868 súvisí s pretečením vyrovnávacej pamäte na halde. Vysoko závažná zraniteľnosť CVE-2026-7354 umožňuje čítať a zapisovať do pamäte mimo povolené hodnoty. Vysoko závažná CVE-2026-7359 umožňuje opätovné použitie dealokovanej pamäte.

Vysoko závažná chyba zabezpečenia CVE-2026-7358 sa nachádza v komponente **Animation** a umožňuje opätovne použiť dealokovanú pamäť.

V komponente **Blink** bola opravená jedna vysoko závažná zraniteľnosť. CVE-2026-5872 umožňuje opätovné použitie dealokovanej pamäte.

Kritická zraniteľnosť CVE-2026-7363 sa nachádza v komponente **Canvas**. Umožňuje opätovné použitie dealokovanej pamäte.

Tri vysoko závažné chyby zabezpečenia CVE-2026-6317, CVE-2026-7338 a CVE-2026-7349 sa nachádzajú v komponente **Cast** a umožňujú opätovné použitie dealokovanej pamäte.

Rovnaký typ zraniteľností bol opravený aj v komponente **Codecs**. Tieto chyby nesú označenie CVE-2026-6303, CVE-2026-6362 a CVE-2026-7348.

Vysoko závažná zraniteľnosť CVE-2026-7360 sa nachádza v komponente **Compositing**. Súvisí s nedostatočným ošetrením nedôveryhodných vstupov.

Komponent **CORS** obsahuje jednu vysoko závažnú zraniteľnosť. CVE-2026-6313 súvisí s nedostatočným presadzovaním nešpecifikovanej bezpečnostnej politiky.

V komponente **CSS** bola opravená vysoko závažná zraniteľnosť CVE-2026-6300, ktorá umožňuje opätovne použiť dealokovanú pamäť.

Komponent **Dawn** obsahuje vysoko závažnú zraniteľnosť, ktorá dovoľuje opätovné použitie dealokovanej pamäte. Zraniteľnosť dostala identifikátor CVE-2026-6310.

Vysoko závažná zraniteľnosť CVE-2026-6919 v komponente **DevTools** dovoľuje opätovné použitie dealokovanej pamäte.

Vysoko závažná zraniteľnosť CVE-2026-7345 v komponente **Feedback** súvisí s nedostatočným overením nedôveryhodných vstupov.

Vysoko závažná zraniteľnosť CVE-2026-6360 v komponente **FileSystem** umožňuje opätovné použitie dealokovanej pamäte.

Rovnaký typ zraniteľnosti bol opravený v komponente **Forms**. Zraniteľnosť dostala označenie CVE-2026-6316.

Komponent **GPU** obsahuje 4 vysoko závažné zraniteľnosti. CVE-2026-6314 a CVE-2026-6920 umožňujú zapisovať a čítať pamäť mimo povolené hodnoty. CVE-2026-7333 a CVE-2026-7357 umožňujú opätovné použitie dealokovanej pamäte.

Komponent **Graphite** obsahuje vysoko závažnú zraniteľnosť CVE-2026-6304, ktorá umožňuje opätovné použitie dealokovanej pamäte. Rovnaký typ zraniteľnosti obsahuje komponent **Chromoting** (vysoko závažná CVE-2026-7347) a **iOS** (kritická CVE-2026-7361).

Komponent **Media** obsahuje 4 vysoko závažné zraniteľnosti. CVE-2026-5866, CVE-2026-6308 a CVE-2026-7335 dovoľujú opätovné použitie dealokovanej pamäte. CVE-2026-6308 umožňuje čítať pamäť mimo povolené hodnoty.

Vysoko závažná zraniteľnosť CVE-2026-7351 v komponente **MHTML** súvisí so vznikom súbehu.

Vysoko závažná zraniteľnosť CVE-2026-7356 v komponente **Navigation** umožňuje opätovné použitie dealokovanej pamäte.

Komponent **Passwords** obsahuje jednu vysoko závažnú zraniteľnosť. CVE-2026-6312 súvisí s nedostatočným presadzovaním nešpecifikovanej bezpečnostnej politiky.

V komponente PDFium sa nachádzajú tri vysoko závažné zraniteľnosti CVE-2026-6305, CVE-2026-6306 a CVE-2026-6361, ktoré súvisia s pretečením vyrovnávacej pamäte na halde.

Vysoko závažná zraniteľnosť CVE-2026-6315 v komponente Permissions umožňuje opätovné použitie dealokovanej pamäte. Rovnaký charakter majú kritické zraniteľnosti CVE-2026-6299 v komponente Prerender a CVE-2026-6297 v komponente Proxy.

Komponent Skia obsahuje jednu kritickú a dve vysoko závažné zraniteľnosti. Kritická chyba zabezpečenia CVE-2026-6298 a vysoko závažná CVE-2026-7353 súvisí s pretečením vyrovnávacej pamäte na halde. CVE-2026-5870 vyplýva z pretečenia celočíselnej premennej.

Vysoko závažná zraniteľnosť CVE-2026-7346 v komponente Tint vyplýva z nevhodnej implementácie nešpecifikovaných prvkov.

Komponent Turbofan obsahuje dve vysoko závažné zraniteľnosti CVE-2026-6301 a CVE-2026-6307, ktoré vyplývajú zo zámeny typu premennej.

Komponent V8 obsahuje 7 vysoko závažných zraniteľností. CVE-2026-5861 umožňuje opätovné použitie dealokovanej pamäte. CVE-2026-5862 a CVE-2026-5863 vyplývajú z nevhodnej implementácie nešpecifikovaných prvkov. CVE-2026-5865, CVE-2026-5871 a CVE-2026-7337 vyplývajú zo zámeny typu premennej. CVE-2026-5873 umožňuje čítať obsah pamäte mimo povolené hodnoty.

Dve vysoko závažné zraniteľnosti v komponente Video (CVE-2026-6302 a CVE-2026-6359) umožňujú opätovné použitie dealokovanej pamäte. Do rovnakej kategórie spadá kritická CVE-2026-7343 a vysoko závažná CVE-2026-7334 v komponente Views, rovnako ako CVE-2026-6309 v komponente Viz.

Vysoko závažná zraniteľnosť CVE-2026-5864 v komponente WebAudio súvisí s pretečením vyrovnávacej pamäte na halde.

Vysoko závažná zraniteľnosť CVE-2026-7350 sa nachádza v komponente WebMIDI. Umožňuje opätovné použitie dealokovanej pamäte.

Komponent WebML obsahuje dve kritické a dve vysoko závažné zraniteľnosti. Kritická CVE-2026-5858 a vysoko závažné CVE-2026-5867 a CVE-2026-5869 súvisia s pretečením vyrovnávacej pamäte na halde. Kritická CVE-2026-5859 súvisí s pretečením celočíselnej premennej.

Tri vysoko závažné chyby zabezpečenia CVE-2026-5860, CVE-2026-7336 a CVE-2026-7341 sa nachádzajú v komponente WebRTC a umožňujú opätovné použitie dealokovanej pamäte. Zraniteľnosť CVE-2026-7342 rovnakej kategórie obsahuje aj komponent WebView.

Kritická zraniteľnosť CVE-2026-6358 v komponente XR umožňuje opätovné použitie dealokovanej pamäte.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows verzie staršej ako 147.0.7727.137/138
- Google Chrome pre Mac verzie staršej ako 147.0.7727.137/138
- Google Chrome pre Linux verzie staršej ako 147.0.7727.137

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 147.0.7727.137/138 a Linux aspoň na verziu 147.0.7727.137.

ZDROJE:

- https://chromereleases.googleblog.com/2026/04
- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_15.html
- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_22.html
- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html

4. ADOBE ACROBAT A READER

V mesiaci apríl spoločnosť Adobe opravila 2 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.

ZRANITEĽNÉ SYSTÉMY:

- Acrobat DC a Acrobat Reader DC pre Windows a Mac verzie 26.001.21411 a staršie

- Acrobat 2024 pre Windows verzie 24.001.30362 a Mac verzie 24.001.30360 a staršie

ODPORÚČANIA:

Odporúčame aktualizáciu aspoň na verziu:

- Acrobat DC a Acrobat Reader DC pre Windows a Mac 26.001.21431
- Acrobat 2024 pre Windows a Mac 24.001.30365

ZDROJE:

- https://helpx.adobe.com/security/security-bulletin.html#acrobat
- https://helpx.adobe.com/security/products/acrobat/apsb26-43.html
- https://helpx.adobe.com/security/products/acrobat/apsb26-44.html

5. FRAMEWORKY

MICROSOFT .NET FRAMEWORK

V mesiaci apríl spoločnosť Microsoft opravila 1 kritickú a 3 vysoko závažné zraniteľnosti vo frameworku .NET.

Kritická zraniteľnosť CVE-2026-23666 v .NET Framework spočíva v nevhodnom spôsobe narábania s výnimkami, resp. nedostatočnej kontrole nešpecifikovaných vstupov. Neautorizovanému vzdialenému útočníkovi umožňuje spôsobiť **nedostupnosť služby (DoS)**.

.NET obsahuje zraniteľnosť CVE-2026-32178, ktorá spočíva v nevhodnom ošetrení špeciálnych znakov. To umožňuje neautorizovanému vzdialenému útočníkovi vykonávať útoky typu **spoofing**.

Kritická zraniteľnosť CVE-2026-32226 v .NET Framework súvisí so vznikom súbehu procesov. To umožňuje neautorizovanému vzdialenému útočníkovi, ktorý súbeh vyhrá, spôsobiť **nedostupnosť služby (DoS)**.

Chyba zabezpečenia .NET, .NET Framework a Visual Studio s označením CVE-2026-33116 súvisí s nesprávnym narábaním so zdrojmi a nevhodným ošetrením vstupov. Vzdialený neautentifikovaný útočník môže dostať systém do nekonečnej slučky, čím spôsobí **nedostupnosť služby (DoS)**.

ZRANITEĽNÉ SYSTÉMY:

- .NET 10.0 installed on Linux
- .NET 10.0 installed on Mac OS
- .NET 10.0 installed on Windows
- .NET 8.0
- .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
- 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-2026-23666
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32178
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32226
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33116

ORACLE JAVA

Spoločnosť Oracle v mesiaci apríl vydala bezpečnostné aktualizácie, ktoré opravujú 3 vysoko závažné zraniteľnosti v rámci Oracle Java SE.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2026-20652 sa nachádza v komponente JavaFX WebKitGTK. Neautentifikovaný vzdialený útočník by mohol zneužiť nevhodný spôsob narábania s pamäťou na **vyvolanie nedostupnosti aplikácie (DoS)**.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2026-22016 sa nachádza v komponente JAXP. Neautentifikovaný vzdialený útočník by ju mohol zneužiť pomocou API a **získať prístup k citlivým dátam**.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2026-34282 sa nachádza v komponente Networking. Neautentifikovaný vzdialený útočník by jej zneužitím cez volania API mohol spôsobiť opakovaný **pád aplikácie (DoS)**.

ZRANITEĽNÉ SYSTÉMY:

- Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26
- Oracle GraalVM for JDK: 17.0.18, 21.0.10
- GraalVM Enterprise Edition: 21.3.17

ODPORÚČANIA:

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

ZDROJE:

- https://www.oracle.com/security-alerts/
- https://www.oracle.com/security-alerts/cpuapr2026.html#AppendixJAVA
- https://access.redhat.com/security/cve/cve-2026-20652
- https://nvd.nist.gov/vuln/detail/CVE-2026-22016
- https://nvd.nist.gov/vuln/detail/CVE-2026-34282

INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

FORTINET OPRAVILA ZNEUŽÍVANÚ KRITICKÚ ZRANITEĽNOSŤ FORTICLIENTEMS

Spoločnosť Fortinet opravila kritickú aktívne zneužívanú zraniteľnosť svojho produktu FortiClientEMS, ktorá umožňuje obísť autentifikáciu a vzdialene vykonávať kód. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ KRITICKÁ ZRANITEĽNOSŤ MODULU WORDPRESS NINJA FORMS – FILE UPLOADS

Vývojári populárneho modulu pre WordPress, Ninja Forms – File Uploads, vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú aktívne zneužívanú kritickú zraniteľnosť. Jej zneužitie umožňuje nahrávanie ľubovoľných súborov na server. Viac informácií na stránke.

ZRANITEĽNOSŤ DOCKER ENGINE UMOŽŇUJE OBÍSŤ KONTROLU AUTORIZÁCIE

Vývojári Docker Engine opravili vysoko závažnú zraniteľnosť modulov AuthZ, ktorá dovoľuje útočníkom obchádzať kontroly autorizácie a vytvárať napríklad privilegované kontajnery. Viac informácií na stránke.

ZRANITEĽNOSŤ APACHE ACTIVEMQ CLASSIC UMOŽŇUJE VYKONÁVANIE KÓDU

Vývojári opravili vysoko závažnú zraniteľnosť v open-source serveri Apache ActiveMQ Classic, ktorá umožňuje vzdialené vykonávanie kódu. Chyba sa v serveri nachádzala 13 rokov. Zraniteľnosť je aktívne zneužívaná. Viac informácií na stránke.

ZRANITEĽNÉ SMEROVAČE SPOLOČNOSTI TP-LINK MÔŽU UMOŽNIŤ ZNEUŽITIE DNS A ODCUDZENIE PRÍSTUPOVÝCH ÚDAJOV

Upozorňujeme organizácie, aby preverili, či sa pri vzdialenom prístupe do interných systémov nepoužívajú zraniteľné alebo nepodporované smerovače SOHO. Podľa varovania FBI a partnerov útočníci zneužívali kompromitované smerovače na zmenu DHCP a DNS nastavení, čím presmerovali DNS dopyty na vlastné prekladače a následne vedeli cielene podvrhnúť odpovede pre vybrané služby. Takto mohli zachytávať prihlasovacie údaje, tokeny a ďalšie citlivé údaje,

najmä ak používateľ pokračoval aj po upozornení na chybu certifikátu. Medzi zneužívané zariadenia patrili aj smerovače TP-Link obsahujúce zraniteľnosť CVE-2023-50224. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ SAP BUSINESS PLANNING AND CONSOLIDATION A SAP BUSINESS WAREHOUSE

Vývojári spoločnosti SAP opravili kritickú zraniteľnosť v produktoch Business Planning and Consolidation a Business Warehouse, ktorá dovoľuje injektovať príkazy SQL. Útočník s nízkymi oprávneniami môže čítať, prepisovať a mazať dáta v databáze. Viac informácií na stránke.

CISCO OPRAVILA KRITICKÉ ZRANITEĽNOSTI V ISE A ISE-PIC

Spoločnosť Cisco opravila štyri kritické zraniteľnosti produktov Identity Services Engine (ISE) a ISE Passive Identity Connector (ISE-PIC). Chyby zabezpečenia umožňujú útočníkom vykonávať systémové príkazy, čítať ľubovoľné súbory, eskalovať oprávnenia na úroveň používateľa root a spôsobovať nedostupnosť zraniteľných uzlov. Viac informácií na stránke.

ZRANITEĽNOSŤ SPLUNK ENTERPRISE A SPLUNK CLOUD PLATFORM UMOŽŇUJE VYKONÁVAŤ KÓD. SPLUNK MCP SERVER ODHAĽUJE TOKENY.

Splunk Enterprise a Splunk Cloud Platform obsahuje zraniteľnosť, ktorá umožňuje útočníkovi s oprávneniami bežného používateľa vzdialene vykonávať kód nahraním škodlivého súboru do dočasného adresára. Zraniteľnosť Splunk MCP Serveru dovoľuje čítať používateľské tokeny vo voľnom texte. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ SGLANG

Platforma SGLang pre multimodálne modely AI obsahuje kritickú zraniteľnosť, ktorá umožňuje podvrhnutím škodlivej chatovej šablóny renderovaciemu procesu spôsobiť vykonanie ľubovoľného vloženého kódu v jazyku Python. Viac informácií na stránke.

BRIDGE:BREAK – SÉRIA ZRANITEĽNOSTÍ OHROZUJE PRIEMYSELNÉ PREVODNÍKY SILEX A LANTRONIX

Tím Forescout Research – Vedere Labs objavil sadu 22 zraniteľností prevodníkov sériovej komunikácie na IP od spoločností Silex a Lantronix. Útočník s prístupom do lokálnej siete ich môže zneužiť na prevzatie kontroly nad dôležitými priemyselnými riadiacimi prvkami obete. Môže napríklad obchádzať prihlásenie, získať administrátorské oprávnenia a vykonávať v ich kontexte systémové príkazy, či získavať citlivé informácie. Zraniteľnosti dostali súhrnný názov BRIDGE:BREAK. Viac informácií na stránke.

PACK2THEROOT: ESKALÁCIA OPRÁVNENÍ V PACKAGEKIT

Red Team z Deutsche Telekom objavil vysoko závažnú zraniteľnosť, ktorá je v manažéri PackageKit prítomná aspoň 12 rokov. Používateľovi s nízkymi oprávneniami umožňuje inštalovať balíky RPM a vykonávať RPM skriptlety s oprávneniami používateľa root. Viac informácií na stránke.

ZRANITEĽNOSŤ GITHUB UMOŽŇUJE VYKONÁVAŤ PRÍKAZY NA SERVERI

Vývojári spoločnosti GitHub opravili vysoko závažnú zraniteľnosť na platformách GitHub Enterprise Server, GitHub Enterprise Cloud a github.com, ktorá umožňovala používateľom s oprávnením vykonávať príkaz git push vzdialene vykonávať ľubovoľné príkazy na hostiteľskom serveri. Viac informácií na stránke.