MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

JÚL 2025

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci júl 6 kritických a 95 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritické zraniteľnosti CVE-2024-36350 a CVE-2024-36357 sa nachádzajú v niektorých **procesoroch** spoločnosti **AMD**. Súvisia s prechodným vykonávaním inštrukcií (transient execution), ktoré môžu **odhaliť** útočníkovi **citlivé informácie**. Prvá zraniteľnosť môže spôsobiť únik údajov z predošlých úložísk, druhá z vyrovnávacej pamäte L1D.

Kritická zraniteľnosť s identifikátorom CVE-2025-47980 v súčasti **Windows Imaging Component** spočíva v **exponovaní citlivých informácií**, ktoré tak môže získať lokálny neautorizovaný útočník. V rámci úspešného zneužitia zraniteľnosti môže útočník čítať časti pamäte na halde.

Zraniteľnosť CVE-2025-47981 v **SPNEGO Extended Negotiation** súvisí s pretečením zásobníka na halde. Neautorizovanému vzdialenému útočníkovi umožňuje **vykonanie kódu** na zraniteľnom systéme. Chybu zabezpečenia možno zneužiť zaslaním špeciálne vytvorených správ na zraniteľný server.

Kritickú zraniteľnosť CVE-2025-48822 v komponente **Windows Hyper-V Discrete Device Assignment** môže neautorizovaný lokálny útočník zneužiť na **vykonanie kódu**. Zraniteľnosť spočíva v možnosti čítania pamäte mimo povolených hodnôt a útočník na jej zneužitie potrebuje presvedčiť používateľa, aby importoval škodlivý súbor INF.

Zraniteľnosť CVE-2025-49735 v komponente **Windows KDC Proxy Service (KPSSVC)** súvisí s možnosťou použitia dealokovanej pamäte. Neautorizovanému útočníkovi umožňuje **vzdialené vykonanie kódu** na zraniteľnom systéme. Pre zneužitie zraniteľnosti potrebuje útočník vyhrať súbeh procesov.

Vysoko závažné zraniteľnosti CVE-2025-47981, CVE-2025-47998, CVE-2025-48805, CVE-2025-48806, CVE-2025-48817, CVE-2025-48822, CVE-2025-48824, CVE-2025-49657, CVE-2025-49663, CVE-2025-49666, CVE-2025-49668, CVE-2025-49669, CVE-2025-49670, CVE-2025-49672, CVE-2025-49673, CVE-2025-49674, CVE-2025-49676, CVE-2025-49688, CVE-2025-49691, CVE-2025-49724, CVE-2025-49729, CVE-2025-49735, CVE-2025-49742 a CVE-2025-

49753 by vzdialený útočník 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, obídenie bezpečnostných prvkov a spoofingové útoky.

ZRANITEĽNÉ SYSTÉMY:

- Remote Desktop client for Windows Desktop
- Windows 10 for 32-bit Systems
- Windows 10 for x64-based Systems
- 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 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems
- Windows 11 Version 22H2 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 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-2024-36350
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-36357
- https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7029.html
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47980
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47981
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-48822
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49735

Koniec podpory pre Windows 10, staršie verzie Windows 11 a Windows Server 2016

Spoločnosť Microsoft tento rok plánovane ukončí podporu pre všetky verzie Windows 10. Po dátume 14. októbra 2025 už tieto produkty nebudú dostávať aktualizácie zabezpečenia, aktualizácie nesúvisiace so zabezpečením, opravy chýb, technickú podporu a ani aktualizácie technického obsahu online.

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

22H2 Enterprise a Education: podpora skončí 14. októbra 2025.
23H2 Home a Pro: Podpora skončí 11. novembra 2025.

23H2 Enterprise a Education: Podpora skončí 10. novembra 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. 24H2.

2. KANCELÁRSKE BALÍKY MICROSOFT OFFICE A OFFICE WEB APPS

Spoločnosť Microsoft vydala v mesiaci júl bezpečnostné aktualizácie, ktoré opravujú 9 kritických a 13 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritické zraniteľnosti **Microsoft Word** s označením CVE-2025-49698 a CVE-2025-49703 súvisia s možnosťou použitia dealokovaného miesta v pamäti. Neautorizovaný útočník ich môže zneužiť na **vykonanie ľubovoľného škodlivého kódu**. Pre jej zneužitie môže vytvoriť škodlivý súbor RTF, ktorý následne otvorí používateľ, alebo ktorého náhľad vygeneruje Preview Pane.

Kritické zraniteľnosti CVE-2025-49695, CVE-2025-49696, CVE-2025-49697 a CVE-2025-49702 v produktoch **Microsoft Office** súvisia s pretečením medzipamäte na halde, možnosťou použitia dealokovaného miesta v pamäti, možnosťou čítania pamäte mimo povolené hodnoty a zámenou typu premennej. Neautentifikovaný útočník ich môže zneužiť na **vykonanie ľubovoľného škodlivého kódu**. Niektoré zraniteľnosti vyžadujú interakciu používateľa. Vektorom útoku na všetky štyri chyby zabezpečenia môže byť aj vygenerovanie náhľadu súboru (Preview Pane).

Kritické zraniteľnosti CVE-2025-49704 a CVE-2025-53770 sa nachádzajú v produktoch **Microsoft SharePoint** a **SharePoint Server**. Prvá umožňuje autentifikovanému útočníkovi **vzdialene vykonávať kód**, pričom druhá autentifikáciu nevyžaduje. Chyby spočívajú v nevhodnej kontrole generovania kódu a deserializácii nedôveryhodných dát. Pre zraniteľnosť CVE-2025-53770 existuje **verejne dostupný exploit**.

Kritická zraniteľnosť CVE-2025-53762 v produkte **Microsoft Purview** spočíva v nevhodne nastavenom zozname vstupov, čo dovoľuje vzdialenému autorizovanému útočníkovi **získať vyššie oprávnenia**. Spoločnosť Microsoft zraniteľnosť opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre jej odstránenie.

Vysoko závažné zraniteľnosti spočívajú v pretečení medzipamäte na halde, možnosti čítania pamäte mimo povolené hodnoty, použití odalokovaného miesta v pamäti, vzniku súbehu procesov, deserializácii nedôveryhodných dát a nevhodnej kontroly prístupov a oprávnení. Predmetné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu, obídenie bezpečnostných prvkov, získanie citlivých informácií, vykonávanie spoofingových útokov** a **eskaláciu privilégií**.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- 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 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 2016 (32-bit edition)
- Microsoft Outlook 2016 (64-bit edition)
- Microsoft PC Manager
- Microsoft PowerPoint 2016 (32-bit edition)
- Microsoft PowerPoint 2016 (64-bit edition)
- Microsoft Purview

- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription Edition
- Microsoft Teams for Android
- Microsoft Teams for Desktop
- Microsoft Teams for iOS
- Microsoft Teams for Mac
- Microsoft Word 2016 (32-bit edition)
- Microsoft Word 2016 (64-bit 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-2025-49695
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49696
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49697
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49698
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49702
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49703
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49704
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53762
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770

Koniec podpory pre Office 2016 a Office 2019

Spoločnosť Microsoft tento rok plánovane zruší podporu pre Office 2016 a Office 2019. Po dátume 14. októbra 2025 už tieto produkty nebudú dostávať 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 júl opravila dve vysoko závažné zraniteľnosti vo webovom prehliadači Microsoft Edge.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2025-49713 spočíva v zámene typu premennej a umožňuje neautorizovanému útočníkovi vzdialene vykonávať kód. Zneužitie zraniteľnosti vyžaduje interakciu zo strany obete, ktorá musí kliknúť na špeciálne vytvorený URL odkaz.

Druhá vysoko závažná zraniteľnosť s identifikátorom CVE-2025-49741 súvisí s možnosťou získania oprávnení cudzieho používateľa. Vzdialený útočník tak môže získať prístup ku citlivým informáciám.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft Edge (Chromium-based) 138.0.7204.96/.97

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-2025-49713
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49741

MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci júl opravila 6 vysoko závažných zraniteľností v línii internetových prehliadačov Firefox a Firefox ESR.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť CVE-2025-8027 súvisiaca s **chybou zápisu do pamäte**. Javascriptový nástroj IonMonkey-JIT zapisuje na haldu iba 32 bitov návratovej 64 bitovej hodnoty, zatiaľ čo Baseline-JIT číta celých 64 bitov.

Zraniteľnosť CVE-2025-8028 v líniách Firefox a Firefox ESR môže zapríčiniť na systémoch s arm64 **chybný výpočet adresy vetvy v pamäti**. Chyba súvisí s tabuľkou WASM br_table. Pokiaľ obsahuje priveľa vstupov, môže byť označenie natoľko vzdialené od inštrukcie, že sa inštrukcia oreže.

Identifikátory CVE-2025-8034, CVE-2025-8035, CVE-2025-8040 a CVE-2025-8044 pokrývajú sadu zraniteľností v líniách Firefox a Firefox ESR, ktoré ovplyvňujú bezpečnosť pamäte a môžu viesť ku **poškodeniu pamäte** alebo možnosti **vykonávať kód**.

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox verzie staršie ako 141
- Mozilla Firefox ESR verzie staršej ako 115.26, 128.13 a 140.1

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 141 a Firefox ESR na verziu 115.26, 128.13 alebo 140.1.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-56/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-57/

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-58/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-59/

GOOGLE CHROME

V mesiaci júl spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 6 vysoko závažných zraniteľností.

CVE-2025-6558 sa nachádza v komponentoch ANGLE a GPU. Súvisí s nesprávnym vyhodnocovaním nedôveryhodných vstupov. Spoločnosť Google informovala, že pre ňu existuje verejne dostupný exploit.

Zneužiť pretečenie celočíselnej premennej umožňuje vysoko závažná zraniteľnosť CVE-2025-7656 v komponente V8. Tento komponent obsahuje tiež zraniteľnosti CVE-2025-8010 a CVE-2025-8011 súvisiace so zámenou typu premennej.

Vysoko závažná zraniteľnosť CVE-2025-7657 v komponente WebRTC umožňuje použitie dealokovaného miesta v pamäti.

Komponent Media Stream obsahuje vysoko závažnú zraniteľnosť CVE-2025-8292, ktorá spočíva v použití dealokovaného miesta v pamäti.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows a Mac verzie staršej ako 138.0.7204.183/.184
- Google Chrome pre Linux verzie staršej ako 138.0.7204.183

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 138.0.7204.183/.184 a Linux verzie aspoň na verziu 138.0.7204.183.

ZDROJE:

- https://chromereleases.googleblog.com/2025/07
- https://chromereleases.googleblog.com/2025/07/stable-channel-update-for-desktop.html

- https://chromereleases.googleblog.com/2025/07/stable-channel-update-for-desktop_15.html
- https://chromereleases.googleblog.com/2025/07/stable-channel-update-for-desktop_22.html
- https://chromereleases.googleblog.com/2025/07/stable-channel-update-for-desktop_29.html

4. ADOBE ACROBAT A READER

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

ZDROJE:

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

5. FRAMEWORKY

MICROSOFT .NET FRAMEWORK

V mesiaci júl spoločnosť Microsoft neopravila žiadnu kritickú ani vysoko závažnú zraniteľnosť vo frameworku .NET.

ZDROJE:

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

ORACLE JAVA

Spoločnosť Oracle v mesiaci júl vydala bezpečnostné aktualizácie, ktoré opravujú 7 vysoko závažných zraniteľností v rámci Oracle Java SE.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2025-50059 sa nachádza v komponente Networking. Neautentifikovaný vzdialený útočník by ju mohol zneužiť na **získanie prístupu k citlivým informáciám**.

Vysoko závažné zraniteľnosti s identifikátormi CVE-2025-30749 a CVE-2025-50106 sa nachádzajú v komponente 2D. Neautentifikovaný vzdialený útočník by ich mohol zneužiť na **získanie úplnej kontroly nad zraniteľnou inštanciou Oracle Java SE, Oracle GraalVM for JDK a Oracle GraalVM Enterprise Edition**.

Vysoko závažná zraniteľnosť CVE-2025-23166 sa nachádza v komponente Node.js. Metóda *SignTraits::DeriveBits()* môže na základe používateľského vstupu nesprávne vyvolať výnimku (funkcia *ThrowException()*). Neautentifikovaný vzdialený útočník by mohol vyvolať **nedostupnosť služby**.

Vysoko závažná zraniteľnosť CVE-2025-27113 súvisí s dereferenciou nulového ukazovateľa v *xmlPatMatch* v *pattern.c* a CVE-2025-24855 v *numbers.c* v *libxslt* dovoľuje použiť dealokované miesto v pamäti. Nachádzajú sa v komponente JavaFX.

Vysoko závažná zraniteľnosť CVE-2025-50063 v komponente Install umožňuje lokálnemu útočníkovi s nízkymi oprávneniami **získanie kontroly nad zraniteľnou inštanciou Oracle Java SE**. Pre úspešné zneužitie zraniteľnosti je potrebná interakcia obete.

ZRANITEĽNÉ SYSTÉMY:

- Oracle Java SE: 8u451, 8u451-perf, 8u451-b50, 11.0.27, 17.0.15, 21.0.7, 24.0.1
- Oracle GraalVM for JDK 17.0.15, 21.0.7, 24.0.1
- GraalVM Enterprise Edition 20.3.17, 21.3.14

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/cpujul2025.html
- https://nvd.nist.gov/vuln/detail/CVE-2025-50059
- https://nvd.nist.gov/vuln/detail/CVE-2025-30749
- https://nvd.nist.gov/vuln/detail/CVE-2025-50106
- https://nvd.nist.gov/vuln/detail/CVE-2025-23166
- https://nvd.nist.gov/vuln/detail/CVE-2025-27113

- https://nvd.nist.gov/vuln/detail/CVE-2025-24855
- https://nvd.nist.gov/vuln/detail/CVE-2025-50063

INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

ZRANITEĽNOSŤ PROTOKOLU BLUETOOTH

Zariadenia Bluetooth, ktoré obsahujú systémy na čipe (SoCs) od spoločnosti Airoha obsahujú zraniteľnosť, ktorá umožňuje čítanie a zápis do pamäte RAM a flash pamäte. Chýbajúca autentifikácia pri moduloch Bluetooth BR/EDR umožňuje útočníkovi komunikovať so zraniteľným zariadením bez párovania so zariadením. Viac informácií na stránke.

ZRANITEĽNOSŤ CITRIX NETSCALER ADC AND NETSCALER GATEWAY

Spoločnosť Citrix Systems varuje pred kritickou zraniteľnosťou v zariadeniach NetScaler ADC a NetScaler Gateway, ak sú nakonfigurované ako brána – t. j. VPN virtuálny server, ICA Proxy, CVPN, RDP Proxy – alebo ako AAA virtuálny server. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ SUDO

Výskumník z Stratascale Cyber Research Unit objavil kritickú zraniteľnosť v softvérovom balíčku sudo, ktorá neoprávnenému používateľovi umožňuje lokálnu eskaláciu privilégií na Unixových a Unixu-podobným operačných systémov. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V CISCO UNIFIED COMMUNICATIONS MANAGER

Zraniteľnosť v produktoch Cisco Unified Communications Manager (Unified CM) a Cisco Unified Communications Manager Session Management Edition (Unified CM SME) môže umožniť neautentifikovanému vzdialenému útočníkovi prihlásiť sa do napadnutého zariadenia ako používateľ root. Viac informácií na stránke.

ZRANITEĽNOSŤ V MODULE FORMINATOR MOŽNO ZNEUŽIŤ NA KOMPROMITÁCIU WORDPRESS

Vývojári modulu WordPress The Forminator Forms vydali bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť. CVE-2025-6463 možno zneužiť na odstránenie súborov redakčného systému a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

KRITICKÚ ZRANITEĽNOSŤ ANTHROPIC MCP INSPECTOR MOŽNO ZNEUŽIŤ NA VZDIALENÉ VYKONANIE KÓDU

Spoločnosť Anthropic vydala bezpečnostné aktualizácie svojho projektu na testovanie a debugovanie MCP (Model Context Protocol) serverov MCP Inspector, ktoré opravujú kritickú zraniteľnosť. CVE-2025-49596 možno zneužiť na vzdialené vykonanie kódu vedúce k úplnému narušeniu dôvernosti, integrity a dostupnosti systému. Viac informácií na stránke.

ZRANITEĽNOSŤ V SERVICENOW NOW PLATFORM MOŽNO ZNEUŽIŤ NA NEOPRÁVNENÝ PRÍSTUP K ÚDAJOM

Spoločnosť ServiceNow vydala bezpečnostné aktualizácie svojej cloudovej manažmentovej platformy Now Platform, ktoré opravujú vysoko závažnú zraniteľnosť. CVE-2025-3648 by neautentifikovaný alebo autentifikovaný útočník mohol zneužiť na získanie prístupu k citlivým údajom. Viac informácií na stránke.

KRITICKÉ BEZPEČNOSTNÉ ZRANITEĽNOSTI V PRODUKTOCH ADOBE

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty After Effects, Substance 3D Viewer, Audition, InCopy , InDesign, Connect , Dimension, Substance 3D Stager, Illustrator, FrameMaker, AEM Forms , AEM Screens a ColdFusion, ktoré opravujú 60 zraniteľností, z čoho 38 je označených ako kritických. Kritické zraniteľnosti by vzdialený útočník mohol zneužiť na obídenie bezpečnostných prvkov, eskaláciu privilégií a vykonanie kódu. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ WEBOVÉHO APLIKAČNÉHO FIREWALLU FORTINET FORTIWEB

Spoločnosť Fortinet vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť vo webovom aplikačnom firewalle Fortinet FortiWeb. CVE-2025-25257 možno zneužiť na vzdialené vykonanie kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V NPM KNIŽNICI MCP-REMOTE UMOŽŇUJE VZDIALENÉ VYKONANIE PRÍKAZOV

Vývojári NPM knižnice mcp-remote vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú kritickú zraniteľnosť. MCP (Model Context Protocol) protokol predstavuje štandard pre integráciu a výmenu dát medzi LLM modelmi a externými dátovými zdrojmi alebo službami. CVE-2025-6514 možno zneužiť na vzdialené vykonanie príkazov operačného systému. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ KRITICKÁ ZRANITEĽNOSŤ VO WING FTP

Vývojári FTP servera Wing FTP vydali bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú kritickú zraniteľnosť. CVE-2025-47812 možno zneužiť na vzdialené vykonanie systémových príkazov a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

WORDPRESS PLUGIN GRAVITY FORMS ZNEUŽITÝ NA ŠÍRENIE ŠKODLIVÉHO KÓDU

Útočníci kompromitovali systémy vývojárov populárneho modulu Gravity Forms pre WordPress a modifikáciou inštalačných súborov zrealizovali útok na dodávateľský reťazec, čím ohrozili všetkých jeho používateľov. Jedná sa o celosvetovo rozšírený plugin, ktorý používajú aj spoločnosti ako Airbnb, Nike, Unicef či Google. Viac informácií na stránke.

ZRANITEĽNOSTI ZARIADENÍ HEWLETT-PACKARD ENTERPRISE NETWORKING INSTANT ON ACCESS POINT

Hewlett-Packard Enterprise (HPE) vydala bezpečnostné aktualizácie pre firmvér zariadení Networking Instant On Access Point, ktoré opravujú jednu kritickú a jednu vysoko závažnú zraniteľnosť. CVE-2025-37103 súvisí s napevno kódovanými prihlasovacími údajmi a CVE-2025-37102 umožňuje vykonávať systémové príkazy. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ ZRANITEĽNOSŤ CRUSHFTP

Vývojári FTP klienta CrushFTP vydali aktualizáciu pre novú zero-day zraniteľnosť, ktorá je aktívne zneužívaná. Útočníkom umožňuje získať administrátorský prístup ku zraniteľným zariadeniam. Viac informácií na stránke.

ZRANITEĽNÁ APLIKÁCIA EXPRESSVPN SMERUJE KOMUNIKÁCIU RDP MIMO TUNEL

ExpressVPN vo svojej poslednej aktualizácii opravila chybu, ktorá spôsobuje, že komunikácia vedúca cez Remote Desktop Protocol neprechádza VPN tunelom. Viac informácií na stránke.