MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

APRÍL 2025

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci apríl 6 kritických a 84 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritické zraniteľnosti s identifikátormi CVE-2025-27480 a CVE-2025-27482 v komponente **Windows Remote Desktop Services** spočívajú v možnosti použitia dealokovaného miesta v pamäti a nedostatočnej ochrane dát v pamäti. To umožňuje **vzdialené vykonanie kódu**. Pre úspešné zneužitie zraniteľností je potrebné, aby útočník vyhral súbeh procesov, ktorý môže vyvolať po pripojení k zariadeniu slúžiacemu ako Remote Desktop Gateway. Útok je možné vykonať v rámci siete bez potreby autentifikácie.

Komponent **Hyper-V** obsahuje zraniteľnosť CVE-2025-27491, ktorá súvisí s možnosťou použitia dealokovaného miesta v pamäti a umožňuje útočníkovi s nízkymi oprávneniami **vzdialene vykonávať kód** v rámci siete. Pre zneužitie zraniteľnosti potrebuje útočník vyhrať súbeh procesov. Potrebuje pri tom presvedčiť obeť, aby pristúpila na škodlivú webovú lokalitu.

Zraniteľnosti s identifikátorom CVE-2025-26670 a CVE-2025-26663 sa nachádzajú v implementácii protokolu **LDAP** a spočívajú v možnosti použitia dealokovaného miesta v pamäti. Vzdialený neautentifikovaný útočník by ju mohol zneužiť na **vzdialené vykonanie kódu**. Pre úspešné zneužitie zraniteľnosti je potrebné, aby útočník vyhral súbeh procesov. Útok je možné vykonať sekvenčne odoslanými špeciálne upravenými požiadavkami na server LDAP.

Implementácia protokolu **TPC/IP** obsahuje kritickú zraniteľnosť CVE-2025-26686, ktorá umožňuje kvôli nedostatočnej ochrane dát v pamäti **vzdialene vykonávať kód**. Neautentifikovaný útočník ju môže zneužiť podvrhnutím falošnej IPv6 adresy v rámci odpovede na požiadavku DHCPv6, ktorú poslala obeť. Útočník potrebuje vyhrať súbeh procesov.

Vysoko závažné zraniteľnosti vo **Windows Server 2016** (CVE-2025-27481, CVE-2025-26671, CVE-2025-26668, CVE-2025-21222), **Windows Server 2025** (CVE-2025-21205, CVE-2025-27729, CVE-2025-26674) a **Windows 10** (CVE-2025-27487, CVE-2025-27477, CVE-2025-26666, CVE-2025-21221) 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 realizáciu spoofingových útokov.

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 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-2025-27480
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27491
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27482
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26670
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26686
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26663

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 apríl bezpečnostné aktualizácie, ktoré opravujú 5 kritických a 17 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritické zraniteľnosti CVE-2025-27745, CVE-2025-27748 a CVE-2025-27749 v produktoch **Microsoft Office** súvisia s možnosťou použitia dealokovaného miesta v pamäti. Neautentifikovaný útočník ich môže zneužiť na **vykonanie ľubovoľného škodlivého kódu**. Na to potrebuje presvedčiť obeť, aby si napríklad stiahla a otvorila špeciálne vytvorený súbor. Útok sa spustí aj prostredníctvom náhľadu súboru (Preview Pane).

Microsoft Excel obsahuje kritické zraniteľnosti CVE-2025-27752 a CVE-2025-29791, ktoré umožňujú **vykonanie ľubovoľného kódu**. Súvisia s pretečením vyrovnávacej pamäte na halde a neoverením typu premennej. Na jej zneužitie potrebuje útočník presvedčiť obeť, aby pristúpila ku špeciálne vytvorenému súboru. Útok sa spustí aj prostredníctvom náhľadu súboru (Preview Pane).

Vysoko závažné zraniteľnosti spočívajú v možnosti čítania mimo povolených hodnôt v pamäti, pretečení celočíselnej premennej, použití odalokovaného miesta v pamäti, dereferencii nedôveryhodného ukazovateľa, deserializácii nedôveryhodných dát, nedostatočnej ochrane citlivých dát a nevhodnej kontroly prístupov a oprávnení. Predmetné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu, eskaláciu privilégií, získanie prístupu k citlivým informáciám** a **obídenie bezpečnostných prvkov**.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft Access 2016 (32-bit edition)

- Microsoft Access 2016 (64-bit edition)
- Microsoft AutoUpdate for Mac
- 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 for Universal
- 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 2016 (32-bit edition)
- Microsoft OneNote 2016 (64-bit edition)
- Microsoft OneNote for Mac
- Microsoft Outlook for Android
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription Edition
- Microsoft Word 2016 (32-bit edition)
- Microsoft Word 2016 (64-bit edition)
- Office Online Server
- SharePoint Server Subscription Edition Language Pack

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-2025-27745
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27748
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27749
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27752
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29791

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 apríl opravila 3 vysoko závažné zraniteľnosti vo webovom prehliadači Microsoft Edge.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2025-25000 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-2025-29815 súvisí s možnosťou použitia dealokovanéo miesta v pamäti. Útočníkovi s nízkymi oprávneniami umožňuje **vzdialene vykonávať kód**. Zneužitie zraniteľnosti vyžaduje interakciu zo strany obete, ktorá musí kliknúť na špeciálne vytvorený URL odkaz. Útočník má následne dosah na citlivé informácie, môže v nich robiť zmeny a spôsobiť pád v rámci tabu prehliadača.

Posledná vysoko závažná zraniteľnosť s identifikátorom CVE-2025-29834 súvisí s možnosťou čítania pamäte mimo povolené hodnoty a tak isto umožňuje **vzdialene vykonávať kód**. Pre jej zneužitie útočník nepotrebuje žiadne oprávnenia, no potrebuje interakciu zo strany obete, ktorá musí kliknúť na špeciálne vytvorený URL odkaz.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft Edge (Chromium-based) 135.0.7049.41/.42/.52

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-2025-25000
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29815
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29834

MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci apríl opravila 9 vysoko závažných zraniteľností v línii internetových prehliadačov Firefox a Firefox ESR.

CVE-2025-3028 v línii Firefox a Firefox ESR umožňuje **použiť dealokované miesto v pamäti**, ak sa vykonáva kód Javascript pri súčasnom spracovaní dokumentu nástrojom XSLTProcessor.

CVE-2025-3608 v línii Firefox v komponente nsHttpTransaction súvisí s možnosťou vyvolať súbeh procesov, ktorý môže byť zneužitý na **poškodenie pamäte a ďalšie útoky**.

Línie Firefox a Firefox ESR obsahujú v aktualizačnom mechanizme prehliadača zraniteľnosť CVE-2025-2817, ktorá umožňuje **získať vyššie oprávnenia**. Umožňuje to nedostatočný kontrolný mechanizmus, ktorý dovoľuje používateľskému procesu interagovať s aktualizačným procesom so systémovou úrovňou oprávnení.

Zraniteľnosť CVE-2025-4082 v línii Firefox a Firefox ESR pre macOS súvisí s chybou v komponente WebGL. Modifikáciou atribútov shaderu je možné vyvolať možnosť **čítania pamäte mimo povolené hodnoty** a v kombinácii s inými zraniteľnosťami **získať vyššie oprávnenia**.

Línie Firefox a Firefox ESR obsahujú vysoko závažnú zraniteľnosť CVE-2025-4083, ktorá súvisí s chybou v izolovaní procesov a nesprávnym narábaním s parametrom „javascript:“. URI v parametri môžu byť vykonané v procese nad zamýšľaným rámcom, čo môže viesť k **úniku zo sandboxu**.

Bližšie nešpecifikované zraniteľnosti s označením CVE-2025-3030 (línie Firefox, Firefox ESR), CVE-2025-3034, CVE-2025-4092 (línia Firefox) a CVE-2025-4093 (línia Firefox ESR) môžu spôsobiť **poškodenie obsahu pamäte** a umožniť **vzdialené vykonanie kódu**.

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox verzie staršie ako 138
- Mozilla Firefox ESR verzie staršej ako 115.23 a 128.10

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 138 a Firefox ESR na verziu 115.23 alebo 128.10.

ZDROJE:

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

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-20/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-21/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-22/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-25/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-28/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-29/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-30/

GOOGLE CHROME

V mesiaci apríl spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 1 kritickú a 3 vysoko závažné zraniteľnosti.

Kritická zraniteľnosť CVE-2025-3619 v komponente Codecs súvisí s pretečením medzipamäte na halde. Útočník môže zneužiť poškodenie dát na halde pomocou špeciálne vytvorenej HTML stránky.

Vysoko závažné zraniteľnosti CVE-2025-3066 v komponente Site Isolation a CVE-2025-3620 v komponente USB súvisí s možnosťou použitia dealokovaného miesta v pamäti. Útočník môže zneužiť poškodenie haldy pomocou špeciálne vytvorenej HTML stránky.

Zneužiť pretečenie medzipamäte na halde umožňuje vysoko závažná zraniteľnosť CVE-2025-4096 v komponente HTML.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows a Mac verzie staršej ako 136.0.7103.48/49
- Google Chrome pre Linux verzie staršej ako 136.0.7103.59

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 136.0.7103.48/49 a Linux verzie aspoň na verziu 136.0.7103.59.

ZDROJE:

- https://chromereleases.googleblog.com/2025/04

- https://chromereleases.googleblog.com/2025/04/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2025/04/stable-channel-update-for-desktop_8.html
- https://chromereleases.googleblog.com/2025/04/stable-channel-update-for-desktop_15.html
- https://chromereleases.googleblog.com/2025/04/stable-channel-update-for-desktop_22.html
- https://chromereleases.googleblog.com/2025/04/stable-channel-update-for-desktop_29.html
- https://nvd.nist.gov/vuln/detail/CVE-2025-3619
- https://nvd.nist.gov/vuln/detail/CVE-2025-3066
- https://nvd.nist.gov/vuln/detail/CVE-2025-3620

4. ADOBE ACROBAT A READER

V mesiaci apríl 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 apríl spoločnosť Microsoft opravila 1 vysoko závažnú zraniteľnosť vo frameworku .NET.

Zraniteľnosť CVE-2025-26682 v ASP.NET Core spočíva v prideľovaní systémových zdrojov bez obmedzení. To umožňuje vzdialenému neautentifikovanému útočníkovi spôsobiť nedostupnosť služby (DoS).

ZRANITEĽNÉ SYSTÉMY:

- ASP.NET Core 8.0
- ASP.NET Core 9.0

ODPORÚČANIA:

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

ZDROJE:

- https://msrc.microsoft.com/update-guide/en-us
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26682

ORACLE JAVA

Spoločnosť Oracle v mesiaci apríl vydala bezpečnostné aktualizácie, ktoré opravujú 4 vysoko závažné zraniteľnosti v rámci Oracle Java SE.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2025-23083 sa nachádza v komponente Node.js v Permission Model. Neautentifikovaný lokálny útočník by ju mohol zneužiť na **manipuláciu eventov** zneužitím nástroja diagnostics_channel.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2024-54534 sa nachádza v komponente JavaFX (WebKitGTK). Neautentifikovaný vzdialený útočník by ju mohol zneužiť na **získanie úplnej kontroly nad zraniteľnou inštanciou Oracle Java SE**.

Vysoko závažná zraniteľnosť CVE-2024-47606 sa nachádza v komponente JavaFX (gstreamer). Vo funkcii qtdemux_parse_theora_extension môže nastať podtečenie celočíselnej premennej. Neautentifikovaný vzdialený útočník by mohol získať kontrolu nad ukazovateľom v pamäti a zneužiť ju na **vykonanie ľubovoľného kódu**.

Vysoko závažná zraniteľnosť CVE-2025-21587 sa nachádza v komponente JSSE. Neautentifikovaný vzdialený útočník ju môže zneužiť pre získanie schopnosti **vytvárať, modifikovať a mazať citlivé údaje**. Zraniteľnosť je možné zneužiť pomocou dát posielaných cez API.

ZRANITEĽNÉ SYSTÉMY:

- Oracle Java SE: 8u441, 8u441-perf, 11.0.26, 17.0.14, 21.0.6, 24
- Oracle GraalVM for JDK 17.0.14, 21.0.6, 24
- GraalVM Enterprise Edition 20.3.17, 21.3.13

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/cpuapr2025.html
- https://nvd.nist.gov/vuln/detail/CVE-2025-23083
- https://nvd.nist.gov/vuln/detail/CVE-2024-47606
- https://nvd.nist.gov/vuln/detail/CVE-2025-21587

6. INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

APPLE VYDALA OPRAVY 213 ZRANITEĽNOSTÍ V IOS, IPADOS A MACOS, AKTUALIZOVALA AJ STARŠIE SYSTÉMY

Spoločnosť Apple vydala aktualizačné balíky pre svoje systémy iOS, iPadOS a macOS, v ktorých opravuje množstvo bezpečnostných chýb. Zároveň aktualizovala aj staršie systémy iOS a iPadOS verzií 15, 16 a 17 a macOS 13 a 14, s cieľom odstrániť aktívne zneužívané zraniteľnosti zverejnené v posledných mesiacoch. Opravy vydala aj pre tvOS a visionOS. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ CRUSHFTP UMOŽŇUJE OBÍSŤ PRIHLASOVANIE

CrushFTP obsahuje aktívne zneužívanú kritickú zraniteľnosť vo svojom autentifikačnom mechanizme, ktorá dovoľuje prihlásiť sa len s uvedením prihlasovacieho mena. Viac informácií na stránke.

VYSOKO ZÁVAŽNÉ ZRANITEĽNOSTI V PRODUKTOCH SPLUNK

Spoločnosť Splunk vydala bezpečnostné aktualizácie na svoje produkty Splunk Enterprise, Splunk Cloud Platform a Splunk Secure Gateway, ktoré opravujú 8 bezpečnostných zraniteľností, z čoho 2 sú označené ako vysoko závažné. CVE-2025-20229 možno zneužiť na vzdialené vykonanie kódu a CVE-2025-20231 na získanie neoprávneného prístupu k citlivým údajom. Aktualizácie taktiež opravujú viacero zraniteľností v komponentoch tretích strán, ktoré sú v rámci produktov využívané. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V ÚLOŽISKÁCH DELL UNITY, DELL UNITYVSA A DELL UNITY XT

Spoločnosť Dell vydala bezpečnostné aktualizácie na svoje úložiská Dell Unity, Dell UnityVSA a Dell Unity XT, ktoré opravujú 15 zraniteľností, z čoho 2 sú označené ako kritické. Kritickú zraniteľnosť s označením CVE-2025-22398 možno zneužiť na vzdialené vykonanie kódu a zraniteľnosť CVE-2025-24383 na vykonanie neoprávnených zmien v systéme, ktoré môžu spôsobiť úplnú nedostupnosť služieb. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V APACHE PARQUET

Vývojári stĺpcovo orientovaného formátu súborov Apache Parquet vydali bezpečnostné aktualizácie pre svoju knižnicu pre Java, ktoré opravujú kritickú zraniteľnosť. CVE-2025-30065 by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémami využívajúcimi predmetnú knižnicu. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ ZRANITEĽNOSŤ V PRODUKTOCH IVANTI ICS, IPS A ZTA GATEWAY

Spoločnosť Ivanti vydala bezpečnostné aktualizácie pre svoje produkty Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS) a ZTA Gateways, ktoré opravujú aktívne zneužívanú kritickú zraniteľnosť. CVE-2025-22457 možno zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

GOOGLE OPRAVIL 2 AKTÍVNE ZNEUŽÍVANÉ ZERO-DAY ZRANITEĽNOSTI OPERAČNÉHO SYSTÉMU ANDROID

Spoločnosť Google vydala bezpečnostné aktualizácie pre svoj operačný systém Android, ktoré opravujú 62 zraniteľností, z čoho 4 je označených ako kritické a 2 ako aktívne zneužívané. CVE-2024-53150 a CVE-2024-53197 v kerneli možno zneužiť na eskaláciu privilégií a získanie neoprávneného prístupu k citlivým údajom. Viac informácií na stránke.

ZRANITEĽNOSŤ APLIKÁCIE WHATSAPP FOR WINDOWS UMOŽŇOVALA VZDIALENÉ VYKONANIE KÓDU

Spoločnosť Meta vydala bezpečnostné aktualizácie pre aplikáciu WhatsApp for Windows, ktoré opravujú bezpečnostnú zraniteľnosť CVE-2025-30401. Napriek tomu, že sa jedná o zraniteľnosť strednej závažnosti, možno ju zneužiť na vzdialené vykonanie škodlivého kódu. Viac informácií na stránke.

ZRANITEĽNOSTI V DATABÁZOVOM SYSTÉME SQLITE

Vývojári databázového systému SQLite vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú dve zraniteľnosti. Ich zneužitím možno vyvolať poškodenie pamäte a zneprístupnenie služby kvôli pádu aplikácie. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V PRODUKTOCH SAP

Spoločnosť SAP vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú 20 zraniteľností, z ktorých 3 sú označené ako kritické. CVE-2025-27429 a CVE-2025-31330 v produktoch SAP S/4HANA a SAP Landscape Transformation možno zneužiť na vzdialené vykonanie kódu. CVE-2025-30016 v produkte SAP Financial Consolidation možno zneužiť na obídenie mechanizmov autentifikácie. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V NÁSTROJI PGADMIN 4

Vývojári nástroja na administráciu databáz PostgreSQL pgAdmin 4 vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú 2 kritické zraniteľnosti. CVE-2025-2946 možno zneužiť na realizáciu XSS útokov a CVE-2025-2945 na vzdialené vykonanie kódu. Viac informácií na stránke.

ZRANITEĽNOSŤ V OPENVPN MOŽNO ZNEUŽIŤ NA ZNEPRÍSTUPNENIE SLUŽBY

Vývojári OpenVPN vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú vysoko závažnú zraniteľnosť. Zraniteľnosť s identifikátorom CVE-2025-2704 možno zneužiť na zneprístupnenie služby. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V ZARIADENIACH FORTINET FORTISWITCH

Spoločnosť Fortinet vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť v zariadeniach FortiSwitch. Zraniteľnosť možno zneužiť na neoprávnenú zmenu prihlasovacích údajov administrátorských účtov a následné získanie úplnej kontroly nad systémom. Viac informácií na stránke.

KRITICKÉ BEZPEČNOSTNÉ ZRANITEĽNOSTI V PRODUKTOCH ADOBE

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty ColdFusion, After Effects, Media Encoder, Bridge, Experience Manager (AEM) Forms on JEE, Premiere Pro, Photoshop, Animate, Experience Manager (AEM) Screens, FrameMaker, XMP-Toolkit-SDK, Commerce, Commerce B2B a Magento Open Source, ktoré opravujú 58 zraniteľností, z čoho 28 je označených ako kritické. Najzávažnejšie kritické zraniteľnosti by vzdialený útočník mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom a vykonanie škodlivého kódu. Viac informácií na stránke.

ACTIVE! MAIL MÁ KRITICKÚ ZERO-DAY ZRANITEĽNOSŤ

Spoločnosť Qualitia opravila kritickú zraniteľnosť v mailovom klientovi Active! Mail, ktorá umožňuje vzdialené vykonávanie kódu. Zraniteľnosť útočníci aktívne zneužívajú. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V SONICWALL SONICOS SSLVPN

Spoločnosť SonicWall vydala bezpečnostné aktualizácie svojho operačného systému SonicOS, ktoré opravujú vysoko závažnú zraniteľnosť v rozhraní SSLVPN Virtual Office. CVE-2025-32818 by vzdialený neautentifikovaný útočník mohol zneužiť na zneprístupnenie služby. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ VO FRAMEWORKU PYTORCH

Vývojári pythonového open-source frameworku pre strojové učenie PyTorch vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú kritickú zraniteľnosť. CVE-2025-32434 možno zneužiť na vzdialené vykonanie kódu. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V KNIŽNICI ERLANG/OTP

Vývojári knižnice Erlang OTP (Open Telecom Platform) vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú kritickú zraniteľnosť v serverovom komponente SSH. Zraniteľnosť s identifikátorom CVE-2025-32433 možno zneužiť na vzdialené vykonanie kódu. Viac informácií na stránke.