MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

JÚN 2025

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci jún 4 kritické a 40 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritická zraniteľnosť CVE-2025-29828 sa nachádza v komponente Windows Schannel (Windows Cryptographic Services) a súvisí s nevhodnou správou pamäte. Zraniteľnosť umožňuje **vzdialené vykonanie kódu**. Neautentifikovaný útočník potrebuje pre zneužitie zraniteľnosti zaslať serveru, ktorý prijíma spojenia TLS, veľké množstvo požiadaviek typu ClientHello.

Kritická zraniteľnosť s identifikátorom CVE-2025-32710 v komponente **Windows Remote Desktop Services** spočíva v použití dealokovaného miesta v pamäti. To umožňuje neautorizovanému útočníkovi **vzdialené vykonanie kódu**. Pre úspešné zneužitie zraniteľnosti potrebuje útočník vykonať pokusy o pripojenie k systému v roli Remote Desktop Gateway a vyhrať súbeh procesov.

Zraniteľnosť CVE-2025-33070 v komponente **Windows Netlogon** súvisí s použitím neinicializovaných zdrojov. Neautorizovanému vzdialenému útočníkovi umožňuje **eskalovať svoje oprávnenia** na zraniteľnom systéme na úroveň doménového administrátora. Zraniteľnosť možno zneužiť zaslaním špeciálne upravených autentifikačných požiadaviek na doménový kontrolér.

Kritickú zraniteľnosť CVE-2025-33071 v komponente **Windows KDC Proxy Service (KPSSVC)** môže neautorizovaný vzdialený útočník zneužiť na **vzdialené vykonanie kódu**. Zraniteľnosť spočíva v použití dealokovaného miesta v pamäti a útočník na jej zneužitie potrebuje vyhrať súbeh procesov.

Vysoko závažné zraniteľnosti CVE-2025-33064, CVE-2025-33066 a CVE-2025-33053 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 a 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 Security App
- 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-2025-29828
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32710
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33070
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33071

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 jún bezpečnostné aktualizácie, ktoré opravujú 7 kritických a 13 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritická zraniteľnosť CVE-2025-32711 v produkte **M365 Copilot** spočíva v možnosti injektovať príkazy, a tým získať **prístup k citlivým údajom**. Spoločnosť Microsoft zraniteľnosť opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre jej odstránenie.

Kritická zraniteľnosť **Microsoft Word** s označením CVE-2025-32717 súvisí s pretečením vyrovnávacej pamäte haldy. Neautorizovaný útočník ju 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-2025-47162, CVE-2025-47164, CVE-2025-47167 a CVE-2025-47953 v produktoch **Microsoft Office** súvisia s pretečením medzipamäte na halde, možnosťou použitia dealokovaného miesta v pamäti, zámenou typu premennej a nedostatočnou ochranou zdrojov. Neautentifikovaný útočník ich môže zneužiť na **vykonanie ľubovoľného škodlivého kódu**. Vektorom útoku môže byť aj vygenerovanie náhľadu súboru (Preview Pane).

Kritická zraniteľnosť CVE-2025-47172 v produkte **Microsoft SharePoint Server** umožňuje autentifikovanému útočníkovi **vzdialene vykonávať kód** pomocou SQL injekcie. Chyba spočíva v nedostatočnej neutralizácii špeciálnych znakov, ktoré môže používateľ zadávať v rámci dotazov SQL.

Vysoko závažné zraniteľnosti spočívajú v pretečení medzipamäte na halde, použití odalokovaného miesta v pamäti, deserializácii nedôveryhodných dát, nedostatočnom ošetrení používateľských dát a nevhodnej kontroly prístupov a oprávnení. Predmetné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu** a **eskaláciu privilégií**.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft 365 Apps for Enterprise for 64-bit Systems

- Microsoft 365 Copilot
- 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 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 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
- 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-2025-32711
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32717
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47162
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47164
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47167
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47953
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47172

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 jún 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 jún opravila 4 vysoko závažné zraniteľnosti v línii internetových prehliadačov Firefox a Firefox ESR.

CVE-2025-49709 v línii Firefox môže viesť pri istých operáciách v komponentoch canvas ku **poškodeniu pamäte**.

CVE-2025-49710 v línii Firefox sa nachádza vo funkcii JavaScript OrderedHashTable. Zraniteľnosť súvisí s **pretečením celočíselnej premennej**.

Línie Firefox a Firefox ESR obsahujú tiež zraniteľnosť CVE-2025-6424. V komponente FontFaceSet môže dôjsť ku **použitiu dealokovanej pamäte**. To môže viesť ku **poškodeniu pamäte**, čo môže byť zneužité pre ďalšie útoky.

Identifikátor CVE-2025-6436 pokrýva sadu zraniteľností ovplyvňujúcich bezpečnosť pamäte, ktoré môžu viesť ku **poškodeniu pamäte** alebo možnosti **vykonávať kód**.

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox verzie staršie ako 140
- Mozilla Firefox ESR verzie staršej ako 115.25 a 128.12

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 140 a Firefox ESR na verziu 115.25 alebo 128.12.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-47/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-51/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-52/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-53/

GOOGLE CHROME

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

Zneužiť možnosť čítania a zápisu do pamäte mimo povolené hodnoty umožňuje vysoko závažná zraniteľnosť CVE-2025-5419 v komponente **V8**. Tento komponent obsahuje tiež zraniteľnosti CVE-2025-5959 súvisiacu so zámenou typu premennej a CVE-2025-6191, ktorá spočíva v pretečení celočíselnej premennej. V8 obsahuje tiež aktívne zneužívanú zraniteľnosť CVE-2025-6554, ktorá spočíva v zámene typu premennej.

Komponent **Media** obsahuje vysoko závažnú zraniteľnosť CVE-2025-5958, ktorá spočíva v použití dealokovaného miesta v pamäti.

Vysoko závažná zraniteľnosť CVE-2025-6192 v komponente **Profiler** vyplýva z možnosti použitia dealokovaného miesta v pamäti.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows verzie staršej ako 138.0.7204.96/.97
- Google Chrome pre Mac verzie staršej ako 138.0.7204.92/.93
- Google Chrome pre Linux verzie staršej ako 138.0.7204.92

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows aspoň na verziu 138.0.7204.96/.97, Mac aspoň na verziu 138.0.7204.92/.93 a Linux verzie aspoň na verziu 138.0.7204.92.

ZDROJE:

- https://chromereleases.googleblog.com/2025/06
- https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_10.html
- https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_17.html
- https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_24.html
- https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_30.html

4. ADOBE ACROBAT A READER

V mesiaci jún spoločnosť Adobe opravila 4 kritické a 6 vysoko závažných zraniteľností v produktoch Adobe Acrobat a Reader.

Kritické zraniteľnosti spočívajúce v použití dealokovaného miesta v pamäti (CVE-2025-43573, CVE-2025-43574, CVE-2025-43576) a zápisu do pamäte mimo povolené hodnoty (CVE-2025-43575) možno zneužiť na **vykonanie ľubovoľného kódu**.

Vysoko závažné zraniteľnosti s označením CVE-2025-43550 a CVE-2025-43577 spočívajú v použití dealokovaného miesta v pamäti a možno ich zneužiť na **vykonanie ľubovoľného kódu**.

Vysoko závažné zraniteľnosti s označením CVE-2025-43578 a CVE-2025-47112 spočívajú v čítaní pamäte mimo povolených hodnôt a možno ich zneužiť na **získanie neoprávneného prístupu k údajom v pamäti**.

Zraniteľnosť CVE-2025-47111 súvisí s dereferenciou nulového ukazovateľa a môže viesť k **odmietnutiu služby aplikácie**.

Obídenie bezpečnostných prvkov dovoľuje zraniteľnosť CVE-2025-43579, ktorá spočíva v exponovanej nešpecifikovanej citlivej informácii.

ZRANITEĽNÉ SYSTÉMY:

- Acrobat DC a Acrobat Reader DC pre Windows a Mac verzie 25.001.20521 a staršie
- Acrobat 2020 a Acrobat Reader 2020 pre Windows a Mac verzie 20.005.30763 a staršie
- Acrobat 2024 pre Windows a Mac verzie 24.001.30235 a staršie

ODPORÚČANIA:

Odporúčame aktualizáciu aspoň na verziu:

- Acrobat DC a Acrobat Reader DC pre Windows 25.001.20531 a Mac 25.001.20529
- Acrobat 2020 a Acrobat Reader 2020 pre Windows a Mac 20.005.30774
- Acrobat 2024 pre Windows a Mac 24.001.30254

ZDROJE:

- https://helpx.adobe.com/security/security-bulletin.html#acrobat
- https://helpx.adobe.com/security/products/acrobat/apsb25-57.html

5. FRAMEWORKY

MICROSOFT .NET FRAMEWORK

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

Zraniteľnosť CVE-2025-30399 v .NET spočíva v možnosti zneužiť nedôveryhodnú vyhľadávaciu cestu na **vzdialené vykonanie kódu** bez potreby autorizácie. Útočník môže obeti podvrhnúť škodlivý súbor, ktorý po nahratí na online alebo lokálny sieťový priečinok a spustení načíta škodlivú knižnicu DLL.

ZRANITEĽNÉ SYSTÉMY:

- .NET 8.0 pre Windows, Linux a MacOS
- .NET 9.0 pre Windows, Linux a MacOS

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-2025-30399

ORACLE JAVA

Spoločnosť Oracle plánuje vydať veľkú sadu opráv 15. júla 2025.

ZDROJE:

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

6. INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

AKTÍVNE ZNEUŽÍVANÉ KRITICKÉ ZRANITEĽNOSTI V PLATFORME VBULLETIN

Bezpečnostní výskumníci zverejnili informácie o aktívne zneužívaných kritických zraniteľnostiach v redakčnom systéme pre tvorbu online fór vBulletin. CVE-2025-48827 a CVE-2025-48828 by vzdialený neautentifikovaný útočník mohol zneužiť na volanie chránených metód a vzdialené vykonanie kódu. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V PRODUKTE HEWLETT PACKARD ENTERPRISE STOREONCE

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostné aktualizácie svojho riešenia pre deduplikáciu, zálohovanie a obnovu dát StoreOnce, ktoré opravujú 8 zraniteľností. Jedna z nich je označená ako kritická. CVE-2025-37093 možno zneužiť na obídenie mechanizmov autentifikácie a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ KRITICKÁ ZRANITEĽNOSŤ V OPEN-SOURCE WEBMAILOVOM RIEŠENÍ ROUNDCUBE

Vývojári populárnej webmailovej platformy Roundcube vydali bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú kritickú zraniteľnosť. CVE-2025-49113 by vzdialený útočník mohol zneužiť na vzdialené vykonanie kódu zaslaním špeciálne vytvorenej požiadavky HTTP GET. Viac informácií na stránke.

VYSOKO ZÁVAŽNÉ ZRANITEĽNOSTI V PRODUKTE IVANTI WORKSPACE CONTROL

Spoločnosť Ivanti vydala bezpečnostné aktualizácie, ktoré opravujú 3 vysoko závažné zraniteľnosti v produkte pre centralizovaný manažment zariadení a aplikácií Ivanti Workspace Control. Zraniteľnosti možno zneužiť na získanie prihlasovacích údajov uložených v aplikácii a úplné narušenie dôvernosti, integrity a dostupnosti systému. Viac informácií na stránke.

KRITICKÉ BEZPEČNOSTNÉ ZRANITEĽNOSTI V PRODUKTOCH ADOBE

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty InCopy, Experience Manager, Commerce, InDesign, Substance 3D Sampler, Acrobat Reader a Substance 3D Painter, ktoré opravujú 252 zraniteľností, z čoho 18 je označených ako kritických. Kritické zraniteľnosti

by vzdialený útočník mohol zneužiť na obídenie bezpečnostných prvkov, eskaláciu privilégií a vykonanie kódu. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V TREND MICRO APEX CENTRAL A ENDPOINT ENCRYPTION POLICYSERVER

Spoločnosť Trend Micro vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viaceré kritické bezpečnostné zraniteľnosti. CVE-2025-49219 a CVE-2025-49220 v Apex Central možno zneužiť na vzdialené vykonanie kódu. CVE-2025-49216, CVE-2025-49212, CVE-2025-49213 a CVE-2025-49217 v Endpoint Encryption PolicyServer možno zneužiť na získanie neoprávneného prístupu do systému a vykonanie kódu. Viac informácií na stránke.

KRITICKÁ A STREDNE ZÁVAŽNÉ ZRANITEĽNOSTI CISCO ISE A CCP S VEREJNÝM EXPLOITOM

Spoločnosť Cisco vydala bezpečnostné aktualizácie na produkty Identity Services Engine a Customer Collaboration Platform, ktoré opravujú viaceré bezpečnostné zraniteľnosti, pre ktoré existuje verejne dostupný kód exploitu. Tieto zraniteľnosti možno zneužiť na získanie neoprávneného prístupu do systému, vykonanie administratívnych zmien, nahrávanie súborov, či získanie citlivých údajov. Viac informácií na stránke.

FEBRUÁROVÉ ZRANITEĽNOSTI V OPERAČNÝCH SYSTÉMOCH APPLE BOLI ZNEUŽITÉ NA INŠTALÁCIU ŠPIONÁŽNEHO SOFTVÉRU

Spoločnosť Apple 11. júna 2025 doplnila popis aktualizácií iOS, iPadOS, macOS Ventura, macOS Sonoma, macOS Sequoia, watchOS a visionOS z 10. februára 2025 o zero-click zraniteľnosť s identifikátorom CVE-2025-43200. Zraniteľnosť bola podľa analýzy The Citizen Lab zneužitá na inštaláciu špionážneho softvéru Graphite od spoločnosti Paragon. Kompromitované mali byť mobilné zariadenia viacerých novinárov v Európe. Viac informácií na stránke.

VYSOKO ZÁVAŽNÁ ZRANITEĽNOSŤ V ASUS ARMOURY CRATE

Spoločnosť ASUS vydala bezpečnostné aktualizácie svojho softvéru pre manažment systému Armoury Crate, ktoré opravujú vysoko závažnú zraniteľnosť. Zraniteľnosť s identifikátorom CVE-2025-3464 možno zneužiť na eskaláciu privilégií a získanie administrátorského prístupu k systému. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V PRODUKTE VEEAM BACKUP & REPLICATION

Spoločnosť Veeam vydala bezpečnostné aktualizácie na svoj produkt Backup & Replication, ktoré opravujú 2 zraniteľnosti, z ktorých jedna je označená ako kritická. CVE-2025-23121 by

vzdialený autentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V CITRIX NETSCALER ADC A NETSCALER GATEWAY

Spoločnosť Citrix vydala bezpečnostné aktualizácie na svoje produkty NetScaler ADC a NetScaler Gateway, ktoré opravujú 2 zraniteľnosti, z ktorých 1 je označená ako kritická. Pravdepodobne aktívne zneužívanú CVE-2025-5777 možno zneužiť na získanie neoprávneného prístupu k citlivým údajom a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V CISCO ISE A ISE-PIC UMOŽŇUJÚ VZDIALENÉ VYKONANIE PRÍKAZOV

Spoločnosť Cisco vydala bezpečnostné aktualizácie pre produkty Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC), ktoré opravujú dve kritické bezpečnostné zraniteľnosti. CVE-2025-20281 a CVE-2025-20282 by útočník mohol zneužiť na vzdialené vykonanie kódu v mene používateľa root a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

ZRANITEĽNOSŤ V INŠTALÁTORE NOTEPAD++ MOŽNO ZNEUŽIŤ NA ESKALÁCIU PRIVILÉGIÍ

Vývojári populárneho textového editora Notepad++ vydali bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť v jeho inštalátore. CVE-2025-49144 možno lokálne zneužiť na eskaláciu privilégií na úroveň SYSTEM a vykonanie kódu. Viac informácií na stránke.

ZRANITEĽNOSŤ VO WINRAR UMOŽŇUJE VZDIALENÉ VYKONANIE KÓDU

Spoločnosť RARLAB vydala bezpečnostné aktualizácie svojho komprimačného nástroja WinRAR, ktoré opravujú vysoko závažnú zraniteľnosť verzií pre Windows. CVE-2025-6218 by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu. Viac informácií na stránke.