MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

MAREC 2025

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci marec 5 kritických a 32 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritické zraniteľnosti s identifikátormi CVE-2025-24035 a CVE-2025-24045 v komponente **Windows Remote Desktop Services** spočívajú v nedostatočnej ochrane dát v pamäti a možnosti použitia dealokovaného miesta v pamäti. To umožňuje **vzdialené vykonanie kódu**. Pre úspešné zneužitie zraniteľností je potrebné, aby útočník vyhral súbeh procesov, ktorý môže vyvolať po pripojení zariadenia s funkciou Remote Desktop Gateway. Útok je možné vykonať v rámci siete bez potreby autentifikácie.

Komponent **Remote Desktop Client** obsahuje zraniteľnosť CVE-2025-26645, ktorá súvisí s možnosťou prechádzania relatívnych ciest a umožňuje neautorizovanému útočníkovi **vzdialene vykonávať kód** v rámci siete. Útočník na to môže zahájiť vzdialené pripojenie z RDS, ktorý má pod kontrolou. Keď sa obeť s administrátorskými oprávneniami pripojí na túto reláciu, útočník získa možnosť vykonávať kód na zraniteľnom klientovi.

Zraniteľnosť s identifikátorom CVE-2025-24064 sa nachádza v službe **DNS Server** a spočíva 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 v rámci siete vhodne načasovaným odoslaním dynamickej aktualizačnej správy pre DNS.

Komponent **Windows Subsystem for Linux (WSL2)** obsahuje kritickú zraniteľnosť CVE-2025-24084, ktorá umožňuje zneužitím dereferencie nedôveryhodného ukazovateľa v pamäti **vykonávať ľubovoľný kód**. Neautentifikovaný útočník ju môže zneužiť zaslaním škodlivého odkazu obeti v rámci e-mailu a lebo správy. Interakcia obete nie je nevyhnutne potrebná.

Vysoko závažné zraniteľnosti vo **Windows Server 2016** (CVE-2025-21180, CVE-2025-24051, CVE-2025-24056 a CVE-2025-24985) a **Windows Server 2019** (CVE-2025-24993) 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 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-2025-24035
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24045
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24064
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24084
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26645

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

Vysoko závažné zraniteľnosti v produktoch **Microsoft Excel 2016** (CVE-2025-24075, CVE-2025-24081 a CVE-2025-24082), **Microsoft Word 2016** (CVE-2025-24078 a CVE-2025-24079), **Microsoft Access 2016** (CVE-2025-26630), **Microsoft Office 2016** (CVE-2025-24057 a CVE-2025-24080), **Microsoft Office LTSC for Mac** (CVE-2025-24077 a CVE-2025-24083) a **Microsoft Office LTSC 2024** (CVE-2025-26629) spočívajú v pretečení medzipamäte zásobníka, pretečení medzipamäte haldy, použití odalokovaného miesta v pamäti a dereferencii nedôveryhodného ukazovateľa. Predmetné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu**.

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 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 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

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 marec opravila 2 vysoko závažné zraniteľnosti vo webovom prehliadači Microsoft Edge.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2025-29795 spočíva v nedostatočnej kontrole odkazov pred prístupom k súborom, na ktoré smerujú. Vzdialený neautentifikovaný útočník by ju mohol zneužiť na **eskaláciu svojich oprávnení** bez interakcie obete.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2025-29806 umožňuje neautorizovanému útočníkovi **vzdialene vykonávať kód** v rámci siete. Zneužitie zraniteľnosti vyžaduje interakciu zo strany obete, ktorá musí kliknúť na špeciálne vytvorený URL odkaz.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft Edge (Chromium-based) 129.0.6668.58/.59

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

MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci marec opravila 2 kritické a 8 vysoko závažných zraniteľností v línii internetových prehliadačov Firefox a Firefox ESR.

Kritickú zraniteľnosť CVE-2024-43097 vo funkcii resizeToAtLeast v komponente SkRegion.cpp je možné zneužiť na **zápis do pamäte mimo povolené hodnoty**. Súvisí s pretečením celočíselnej premennej a je prítomná v líniách Firefox, aj Firefox ESR.

Kritickú zraniteľnosť CVE-2025-2857 v línii Firefox dokáže útočník zneužiť pomocou nešpecifikovaného procesu potomka tak, aby cez jeho rodičovský proces spôsobil **únik zo sandboxu** prehliadača.

Bližšie nešpecifikované zraniteľnosti s označením CVE-2025-1937 a CVE-2025-1938 (línie Firefox, Firefox ESR) a CVE-2025-1943 (línia Firefox) môžu spôsobiť **poškodenie obsahu pamäte** a umožniť **vzdialené vykonanie kódu**.

CVE-2025-1930 v línii Firefox a Firefox ESR pre Windows umožňuje použiť dealokované miesto v pamäti v rámci procesu Browser a **uniknúť zo sandboxu prehliadača**. Zraniteľnosť je možné zneužiť odoslaním špeciálne upravených dát StreamData do komponentu AudioIPC.

CVE-2025-1931 v línii Firefox a Firefox ESR umožňuje použiť dealokované miesto v pamäti v rámci procesu WebTransport.

Línie Firefox a Firefox ESR obsahujú vo funkcii txNodeSorter komponentu XSLT zraniteľnosť CVE-2025-1932, ktorá umožňuje **pristupovať k pamäti mimo povolené hodnoty**.

Zraniteľnosť CVE-2025-1933 v línii Firefox a Firefox ESR súvisí s chybami pri kompilácii WASM i32 v komponente JIT. Výsledné hodnoty môžu byť ovplyvnené zvyškovým obsahom pamäte a môže dôjsť ku **zámene typu premennej**.

Komponent Custom Tabs umožňuje používať aplikáciám pre Android prechodové animácie pri načítaní webstránok. Tieto môžu útočníci zneužiť na prekrytie dialógového okna a oklamanie používateľa pri klikaní na voľby v ňom. Tak môžu napríklad **získať vyššie oprávnenia**. Zraniteľnosť má označenie CVE-2025-1939 a nachádza sa v línii Firefox.

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox verzie staršie ako 136.0.4
- Mozilla Firefox ESR verzie staršej ako 115.21.1 a 128.8.1

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 136.0.4 a Firefox ESR na verziu 115.21.1 alebo 128.8.1.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-14/

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-16/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-19/

GOOGLE CHROME

V mesiaci marec spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 1 kritickú a 5 vysoko závažných zraniteľností.

Kritická zraniteľnosť CVE-2025-2476 v komponente **Lens** umožňuje **použiť dealokované miesto v pamäti**. Útočník ju môže zneužiť poškodením dát na halde pomocou špeciálne vytvorenej HTML stránky.

Aktívne zneužívaná zraniteľnosť CVE-2025-2783 v komponente **Mojo** v Chrome pre Windows OS umožňuje **únik zo sandboxu** prehliadača kvôli logickej chybe na rozhraní prehliadača.

Zraniteľnosti v komponente **V8** spočívajú v **absentujúcom overovaní typu premennej** (CVE-2025-1920, CVE-2025-2135) a **čítaní pamäte mimo povolené hodnoty** (CVE-2025-1914). Útočník ich môže zneužiť pomocou špeciálne vytvorenej webstránky.

Zápis do pamäte mimo povolené hodnoty dovoľuje zraniteľnosť CVE-2025-24201 v komponente GPU v Chrome pre Mac. Útočník ju môže zneužiť pre **únik zo sandboxu** prehliadača. Pre zraniteľnosť existuje verejne dostupný exploit.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows a Mac verzie staršej ako 134.0.6998.177/.178
- Google Chrome pre Linux verzie staršej ako 134.0.6998.165

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 134.0.6998.177/.178 a Linux verzie aspoň na verziu 134.0.6998.165.

ZDROJE:

- https://chromereleases.googleblog.com/2025/03
- https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop.html

- https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_10.html
- https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_19.html
- https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_21.html
- https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_25.html
- https://nvd.nist.gov/vuln/detail/CVE-2025-2476
- https://nvd.nist.gov/vuln/detail/CVE-2025-1920
- https://nvd.nist.gov/vuln/detail/CVE-2025-1914
- https://nvd.nist.gov/vuln/detail/CVE-2025-24201

4. ADOBE ACROBAT A READER

V mesiaci marec spoločnosť Adobe opravila 6 kritických a 3 vysoko závažné zraniteľnosti v produktoch Adobe Acrobat a Reader.

Kritické zraniteľnosti spočívajúce v použití dealokovaného miesta v pamäti (CVE-2025-27174, CVE-2025-27159, CVE-2025-27160), prístupe k neinicializovanému ukazovateľu (CVE-2025-27158, CVE-2025-27162) a čítaní pamäte mimo povolené hodnoty (CVE-2025-27161) možno zneužiť na vykonanie ľubovoľného kódu.

Vysoko závažná zraniteľnosť s označením CVE-2025-24431 spočíva v čítaní pamäte mimo povolených hodnôt a možno ju zneužiť na vykonanie ľubovoľného kódu.

Vysoko závažné zraniteľnosti s označením CVE-2025-27163 a CVE-2025-27164 spočívajú v čítaní pamäte mimo povolených hodnôt a možno ich zneužiť na získanie neoprávneného prístupu k údajom v pamäti.

ZRANITEĽNÉ SYSTÉMY:

- Acrobat DC a Acrobat Reader DC pre Windows a Mac verzie 25.001.20428 a staršie
- Acrobat 2020 a Acrobat Reader 2020 pre Windows a Mac verzie 20.005.30748 a staršie
- Acrobat 2024 pre Windows a Mac verzie 24.001.30225 a staršie

ODPORÚČANIA:

Odporúčame aktualizáciu aspoň na verziu:

- Acrobat DC a Acrobat Reader DC pre Windows a Mac 25.001.20432
- Acrobat 2020 a Acrobat Reader 2020 pre Windows a Mac 20.005.30763
- Acrobat 2024 pre Windows a Mac 24.001.30235

ZDROJE:

- https://helpx.adobe.com/security/products/acrobat/apsb25-14.html

5. FRAMEWORKY

MICROSOFT .NET FRAMEWORK

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

Zraniteľnosť CVE-2025-24070 spočíva v nedostatočne zabezpečených mechanizmoch autentifikácie v ASP.NET Core & Visual Studio a možno ju zneužiť na **eskaláciu privilégií** na úroveň kompromitovaného používateľa.

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-2025-24070

ORACLE JAVA

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

ZDROJE:

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

6. INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

BROADCOM ODSTRÁNIL AKTÍVNE ZNEUŽÍVANÉ ZRANITEĽNOSTI VIRTUALIZAČNEJ PLATFORMY VMWARE

Spoločnosť Broadcom vydala bezpečnostné aktualizácie na svoje virtualizačné platformy VMware ESXi, Workstation a Fusion ktoré opravujú 3 aktívne zneužívané zero-day zraniteľnosti, z čoho jedna je označená ako kritická. Viac informácií na stránke.

ZRANITEĽNOSŤ KNIŽNICE PDFKIT PRE PYTHON

Bezpečnostní analytici CSIRT.SK objavili zraniteľnosť CVE-2025-26240 v knižnici pdfkit v jazyku Python spočíva v metóde from_string, ktorá spracúva používateľské vstupy HTML, ktoré však neošetruje. Metóda from_string používa metaznačky, ktorých názvy začínajú na "pdfkit-", a ich hodnoty konvertuje na parametre príkazového riadku pre nástroj wkhtmltopdf. Túto analýzu vstupov vykonáva metóda _find_options_in_meta, ktorá sa nachádza v súbore pdfkit/pdfkit.py. Hoci táto funkcia môže byť v určitých prípadoch užitočná (napríklad nastavenie veľkosti papiera), niektoré argumenty wkhtmltopdf predstavujú bezpečnostné riziko. 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 44 zraniteľností, z čoho 10 je označených ako kritické a 2 ako aktívne zneužívané. CVE-2024-43093 v komponente Framework a CVE-2024-50302 v komponente HID USB možno zneužiť na získanie neoprávneného prístupu k citlivým údajom v systémových priečinkoch a kernel pamäti. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ KRITICKÁ ZRANITEĽNOSŤ V IP KAMERÁCH EDIMAX IC-7100

Bezpečnostní výskumníci zverejnili informácie o aktívne zneužívanej kritickej zraniteľnosti v IP kamerách Edimax IC-7100 (produkt s ukončenou podporou). Zraniteľnosť s identifikátorom CVE-2025-1316 možno zneužiť na vzdialené vykonanie kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Viac informácií na stránke.

ČIPY ESPRESSIF ESP32 OBSAHUJÚ NEZDOKUMENTOVANÉ FUNKCIE

Bezpečnostní výskumníci zo spoločnosti Tarlogic zverejnili informácie o existencii nezdokumentovaných funkcií v čipoch ESP32, ktoré sú súčasťou veľkého množstva inteligentných a IoT (Internet of Things) zariadení po celom svete. CVE-2025-27840 by útočník s fyzickým prístupom mohol zneužiť na vykonanie neoprávnených zmien v systéme a získanie úplnej kontroly nad zariadeniami. Spoločnosť Espressif sa vyjadrila, že sa jedná o príkazy pre účely interného testovania a nie bezpečnostnú zraniteľnosť. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ ZERO-DAY ZRANITEĽNOSŤ V OPERAČNÝCH SYSTÉMOCH APPLE

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje operačné systémy iOS, iPadOS, macOS Sequoia, visionOS a webový prehliadač Safari, ktoré opravujú aktívne zneužívanú zero-day zraniteľnosť. Zraniteľnosť CVE-2025-24201 v komponente WebKit by útočník podvrhnutím špeciálne vytvoreného webového obsahu mohol zneužiť na únik z Web Content sandboxu a vzdialené vykonanie kódu. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V PRIEMYSELNÝCH SWITCHOCH MOXA

Spoločnosť Moxa vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť v priemyselných switchoch série PT a EDS-508A. CVE-2024-12297 by vzdialený útočník mohol zneužiť na realizáciu útokov na báze brute-force a MD5 kolízií, obídenie mechanizmov autentifikácie a získanie neoprávneného prístupu do systému. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ ZRANITEĽNOSŤ V POPULÁRNEJ SOFTVÉROVEJ KNIŽNICI FREETYPE

Vývojári populárnej open-source softvérovej knižnice pre vykresľovanie fontov FreeType vydali bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú zraniteľnosť vysokej závažnosti. CVE-2025-27363 by vzdialený neautentifikovaný útočník podvrhnutím špeciálne vytvorených súborov mohol zneužiť na vzdialené vykonanie kódu. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V GITLAB MOŽNO ZNEUŽIŤ NA IMPERSONÁCIU POUŽÍVATEĽOV A VYKONANIE KÓDU

Vývojári platformy GitLab vydali bezpečnostné aktualizácie, ktoré opravujú 9 zraniteľností, z čoho 3 sú označené ako kritické. CVE-2025-25291, CVE-2025-25292 v externej knižnici ruby-saml by vzdialený autentifikovaný útočník mohol zneužiť na impersonáciu ľubovoľných používateľov v rámci SAML IdP (Identity Provider) daného prostredia. CVE-2025-27407 v knižnici graphql možno zneužiť na vzdialené vykonanie kódu. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ ZRANITEĽNOSŤ V OPERAČNOM SYSTÉME JUNIPER JUNOS OS

Spoločnosť Juniper vydala bezpečnostné aktualizácie pre svoj sieťový operačný systém Junos OS, ktoré opravujú aktívne zneužívanú zraniteľnosť. CVE-2025-21590 by lokálny útočník s prístupom k shell-u mohol zneužiť na obídenie bezpečnostného mechanizmu Veriexec, vykonanie škodlivého kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ MODULU WORDPRESS GHOST

V module WordPress Ghost bola opravená kritická zraniteľnosť, ktorá umožňuje vzdialene vykonávať kód. Chyba spočíva v možnosti vykonávať útoky typu LFI manipuláciou odkazu URL. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ NEXT.JS

Framework Next.js obsahuje kritickú zraniteľnosť, ktorá umožňuje útočníkom obísť kontroly autorizácie pomocou špeciálne vytvorených požiadaviek, ak prebiehajú v Middleware a ďalej už nie. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ VEEAM BACKUP & REPLICATION

Spoločnosť Veeam opravila kritickú zraniteľnosť v produkte Backup & Replication, ktorá umožňuje útočníkovi s oprávneniami doménového používateľa vzdialene vykonávať kód na serveri Backup Server. Viac informácií na stránke.

VMWARE TOOLS PRE WINDOWS UMOŽŇUJE OBÍSŤ AUTENTIFIKÁCIU

Vývojári VMware Tools pre Windows opravili vo svojom produkte zraniteľnosť vysokej závažnosti, ktorá umožňuje obídenie autentifikácie a získanie oprávnení administrátora pre isté úkony v rámci kompromitovaného virtuálneho prostredia. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ TLAČIARNÍ CANON

Spoločnosť Canon opravila kritickú zraniteľnosť v ovládačoch viacerých svojich zariadení, ktorá umožňuje znefunkčniť tlač, a potenciálne vykonať ľubovoľný kód. Viac informácií na stránke.