MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

OKTÓBER 2025

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci október 3 kritické a 130 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritickú zraniteľnosť CVE-2016-9535 v súčasti tif_predict.h a tif_predict.c knižnice **LibTIFF** môže neautorizovaný lokálny útočník zneužiť na **vykonanie ľubovoľného kódu**. Zraniteľnosť spočíva v možnosti vyvolať zlyhanie niektorých prvkov v debugovacom móde a pretečenie vyrovnávacej pamäte v produkčnom móde. Útočník ju môže zneužiť podvrhnutím dát YCbCr s nezvyčajnou veľkosťou zraniteľným funkciám.

Súčasť **Windows Graphics Component** obsahuje kritickú zraniteľnosť s identifikátorom CVE-CVE-2025-49708. Súvisí s nesprávnou inicializáciou zdrojov a možnosťou použitia dealokovaného miesta v pamäti po výhre súbehu. Vzdialený útočník s nízkymi oprávneniami ju môže zneužiť na **navýšenie svojich oprávnení** na úroveň **SYSTEM**. Útočník s prístupom ku virtuálnemu stroju môže získať prístup do hostiteľského systému.

Kritická zraniteľnosť s identifikátorom CVE-2025-59287 v komponente súčasti **Windows Server Update Service (WSUS)** spočíva v deserializácii nedôveryhodných dát. Vzdialený neautorizovaný útočník ju môže zneužiť na **vzdialené vykonanie kódu**. O zraniteľnosti sme informovali aj na našom webe.

Vysoko závažné zraniteľnosti CVE-2025-54957, CVE-2025-55326, CVE-2025-58718, CVE-2025-58730, CVE-2025-58731, CVE-2025-58732, CVE-2025-58733, CVE-2025-58734, CVE-2025-58735, CVE-2025-58736, CVE-2025-58737, CVE-2025-58738, CVE-2025-59282 a CVE-2025-59295 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, vykonávanie spoofingových útokov, neoprávnené zásahy do systému a obídenie bezpečnostných prvkov.

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 11 Version 25H2 for ARM64-based Systems
- Windows 11 Version 25H2 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-2016-9535
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49708
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287

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. **Po rokovaní s organizáciou Euroconsumers však v Európskom hospodárskom priestore predĺži bezplatnú podporu systémov Windows 10 o rok, teda do októbra 2026. Podmienkou môže byť prihlásenie sa cez Microsoft account.**

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

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 október bezpečnostné aktualizácie, ktoré opravujú 6 kritických a 16 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritické zraniteľnosti CVE-2025-59227 a CVE-2025-59234 v balíkoch **Microsoft Office Imaging Component** môže neautorizovaný lokálny útočník zneužiť na **vykonanie ľubovoľného škodlivého kódu**. Zraniteľnosti spočívajú v možnosti použitia dealokovaného miesta v pamäti a útočník na ich zneužitie potrebuje presvedčiť obeť, aby otvorila škodlivý súbor. Pre jej zneužitie môže slúžiť aj vygenerovanie náhľadu súboru (Preview Pane).

Kritická zraniteľnosť **Microsoft Excel** s označením CVE-2025-59236 súvisí s možnosťou použitia dealokovaného miesta v pamäti. Neautorizovaný útočník ich môže zneužiť na lokálne **vykonanie ľubovoľného škodlivého kódu**. Nepotrebuje na to interakciu obete.

Kritické zraniteľnosti CVE-2025-59252, CVE-2025-59272 a CVE-2025-59286 sa nachádzajú v produktoch **Copilot** a **M365 Copilot**. Súvisia s nevhodným spôsobom sanitizácie príkazov a umožňujú injektovanie škodlivých príkazov. Neautorizovaný vzdialený útočník ich môže zneužiť pri **spoofingových útokoch**. Spoločnosť Microsoft zraniteľnosti opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre ich odstránenie.

Vysoko závažné zraniteľnosti spočívajú v zámene typu premennej, možnosti čítania medzipamäte mimo povolené hodnoty, použití dealokovaného miesta v pamäti, deserializácii nedôveryhodných dát, neošetrenej výnimke a nedostatočnom overení vstupných dát vrátane externých zdrojov. Predmetné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu, získanie citlivých informácií, eskaláciu privilégií** a **zneprístupnenie služby (DoS)**.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft 365 Apps for Enterprise for 32-bit Systems

- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft 365 Copilot's Business Chat
- Microsoft 365 Word Copilot
- 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 Mesh for Meta Quest
- Microsoft Mesh PC Applications
- 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 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-2025-59227
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59234
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59236
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59252
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59272
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59286

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 október 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 október opravila 8 vysoko závažných zraniteľností v línii internetových prehliadačov Firefox a Firefox ESR.

Línie Firefox a Firefox ESR obsahujú zraniteľnosti CVE-2025-11708 súvisiacu možnosťou použitia dealokovanej pamäte vo funkcii MediaTrackGraphImpl::GetInstance().

Zraniteľnosť CVE-2025-11709 línií Firefox a Firefox ESR umožňuje **čítať obsah pamäte a zapisovať do nej mimo povolené hodnoty** v rámci privilegovaného procesu. Útočník na to mohol zneužiť kompromitovaný proces s nižšími privilégiami vzhľadom na cieľový proces a škodlivo upravené textúry WebGL.

Línie Firefox a Firefox ESR obsahujú zraniteľnosti CVE-2025-11710, vedúcu k **úniku citlivých informácií** z pamäte privilegovaného procesu. Útočník na to mohol zneužiť kompromitovaný proces a škodlivé správy IPC.

Zraniteľnosť CVE-2025-11711 v líniách Firefox a Firefox ESR poskytuje možnosť **meniť vlastnosti objektov JavaScript**, ktoré nemajú byť prepisovateľné.

Zraniteľnosť CVE-2025-12380 v línii Firefox súvisí s možnosťou použitia dealokovanej pamäte v komponente WebGPU. Útočník mohol zneužiť kompromitovaný proces potomka na **únik zo sandboxu** tohto procesu.

Identifikátory CVE-2025-11714 a CVE-2025-11715 pokrývajú sadu zraniteľností v líniách Firefox a Firefox ESR a CVE-2025-11721 v línii Firefox. Tieto zraniteľnosti ovplyvňujú bezpečnosť pamäte a môžu viesť ku **poškodeniu pamäte** alebo možnosti **vykonávať kód**.

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox a Firefox pre iOS verzie staršie ako 144.0.2
- Mozilla Firefox ESR verzie staršej ako 115.29 a 140.4

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 144.0.2 a Firefox ESR na verziu 115.29 alebo 140.4.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-81/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-82/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-83/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-86/

GOOGLE CHROME

V mesiaci október spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 10 vysoko závažných zraniteľností.

Komponent V8 obsahuje viacero vysoko závažných zraniteľností. CVE-2025-12428 súvisí so zámenou typu premennej. CVE-2025-12429, CVE-2025-12433 a CVE-2025-12036 sú zapríčinené nevhodnou implementáciou nešpecifikovaných funkcionalít. Zraniteľnosť CVE-2025-12432 je možné zneužiť výhrou súbehu procesov.

Vysoko závažná zraniteľnosť CVE-2025-11458 v komponente Sync je zapríčinená pretečením medzipamäte haldy.

Vysoko závažná zraniteľnosť CVE-2025-11460 v komponente Storage dovoľuje použiť dealokované miesto v pamäti. Rovnaký typ zraniteľnosti obsahuje aj komponent Safe Browsing (CVE-2025-11756).

Komponent Media obsahuje vysoko závažnú zraniteľnosť, ktorá spočíva v chybe v rámci životného cyklu objektu. Bol jej priradený identifikátor CVE-2025-12430.

Vysoko závažná zraniteľnosť CVE-2025-12431 v komponente Extensions vyplýva z nevhodnej implementácie nešpecifikovaných prvkov.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows verzie staršej ako 142.0.7444.59/60
- Google Chrome pre Mac verzie staršej ako 142.0.7444.60
- Google Chrome pre Linux verzie staršej ako 142.0.7444.59

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows aspoň na verziu 142.0.7444.59/60, Mac aspoň na verziu 142.0.7444.60 a Linux aspoň na verziu 142.0.7444.59.

ZDROJE:

- https://chromereleases.googleblog.com/2025/10
- https://chromereleases.googleblog.com/2025/10/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2025/10/stable-channel-update-for-desktop_9.html
- https://chromereleases.googleblog.com/2025/10/stable-channel-update-for-desktop_14.html
- https://chromereleases.googleblog.com/2025/10/stable-channel-update-for-desktop_21.html
- https://chromereleases.googleblog.com/2025/10/stable-channel-update-for-desktop_28.html

4. ADOBE ACROBAT A READER

V mesiaci október 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 október spoločnosť Microsoft opravila 3 vysoko závažné zraniteľnosti vo frameworku .NET.

Zraniteľnosť CVE-2025-55247 v .NET spočíva v možnosti zneužiť nedôveryhodnú vyhľadávaciu cestu na **eskalovanie oprávnení**. Lokálny útočník s nízkymi oprávneniami môže obeti podvrhnúť škodlivý súbor do hlavnej cesty projektu, ktorý mu po vytvorení či zakomponovaní do projektu umožní získať jej oprávnenia.

Vysoko závažná zraniteľnosť CVE-2025-55248 v .NET, .NET Framework a Visual Studio súvisí so slabým šifrovaním. Útočník s nízkymi oprávneniami ju môže v rámci siete zneužiť pre **získanie citlivých osobných informácií**. Na to potrebuje presvedčiť obeť, aby otvorila škodlivý e-mail.

Posledná vysoko závažná zraniteľnosť CVE-2025-55315 v ASP.NET Core dovoľuje vzdialenému útočníkovi s nízkymi oprávneniami **obísť bezpečnostné prvky**. Vyplýva z nekonzistentnej interpretácie požiadaviek HTTP. Útočník potrebuje poslať serveru špeciálne upravenú požiadavku.

ZRANITEĽNÉ SYSTÉMY:

- .NET 8.0 pre Windows, Linux a MacOS
- .NET 9.0 pre Windows, Linux a MacOS
- ASP.NET Core 2.3
- ASP.NET Core 8.0
- ASP.NET Core 9.0
- Microsoft .NET Framework 2.0 Service Pack 2
- Microsoft .NET Framework 3.0 Service Pack 2
- Microsoft .NET Framework 3.5 / 3.5.1
- Microsoft .NET Framework 4.6.2
- Microsoft .NET Framework 4.7 / 4.7.1 / 4.7.2
- Microsoft .NET Framework 4.8 / 4.8.1

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-2025-55247
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-55248
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-55315

ORACLE JAVA

Spoločnosť Oracle v mesiaci október vydala bezpečnostné aktualizácie, ktoré opravujú 2 vysoko závažné zraniteľnosti v rámci Oracle Java SE.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2025-31257 sa nachádza v komponente JavaFX WebKitGTK. Neautentifikovaný vzdialený útočník by mohol zneužiť dealokované miesto v pamäti pre **vyvolanie pádu aplikácie**. Na to potrebuje presvedčiť obeť, aby pristúpila ku škodlivému webovému obsahu

Vysoko závažná zraniteľnosť CVE-2025-53066 sa nachádza v komponente JAXP. Neautentifikovaný vzdialený útočník by ju mohol zneužiť na **získanie úplnej kontroly nad zraniteľnou inštanciou Oracle Java SE, Oracle GraalVM for JDK a Oracle GraalVM Enterprise Edition** a **získať citlivé informácie**.

ZRANITEĽNÉ SYSTÉMY:

- Oracle Java SE: 8u461-b50, 8u461, 8u461-perf, 11.0.28, 17.0.16, 21.0.8, 25
- Oracle GraalVM for JDK: 17.0.16, 21.0.8
- GraalVM Enterprise Edition: 21.3.15

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/cpuoct2025.html
- https://access.redhat.com/security/cve/cve-2025-31257
- https://nvd.nist.gov/vuln/detail/CVE-2025-53066

INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

SOLARWINDS VYDÁVA UŽ TRETIU AKTUALIZÁCIU NA OPRAVU KRITICKEJ ZRANITEĽNOSTI V WEB HELP DESK

Spoločnosť SolarWinds vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť v produkte Web Help Desk. CVE-2025-26399 možno zneužiť na vzdialené vykonanie príkazov a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

NOVÝ FIRMVÉR PRE ZARIADENIA SONICWALL SMA 100 DOKÁŽE ODSTRÁNIŤ ZNÁME ROOTKITY

Spoločnosť SonicWall vydala aktualizáciu firmwaru pre svoje zariadenia série SMA 100, ktorá zavádza pokročilú kontrolu integrity súborov a dokáže identifikovať a odstrániť známe rootkity. Hackerská skupina UNC6148 zneužívala zraniteľnosti webového servera Apache CVE-2024-38475 a SMA 100 CVE-2025-40599 na šírenie rootkitu OVERSTEP. Viac informácií na stránke.

ZRANITEĽNOSTI V SUPERMICRO BMC MOŽNO ZNEUŽIŤ NA MODIFIKÁCIU FIRMVÉRU

Spoločnosť Supermicro vydala bezpečnostné aktualizácie firmvéru BMC (Baseboard Management Controller), ktoré opravujú dve zraniteľnosti vysokej závažnosti. CVE-2025-7937 a CVE-2025-6198 by vzdialený útočník mohol zneužiť na modifikáciu firmvéru zariadenia a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

CISCO OPRAVILO AKTÍVNE ZNEUŽÍVANÚ ZRANITEĽNOSŤ OPERAČNÝCH SYSTÉMOV IOS A IOS XE

Spoločnosť Cisco vydala bezpečnostné aktualizácie, ktoré opravujú 14 zraniteľností operačných systémov Cisco IOS a IOS XE, z čoho jedna je označená ako aktívne zneužívaná zero-day. CVE-2025-20352 by vzdialený útočník mohol zneužiť na zneprístupnenie služby, vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

ZRANITEĽNOSŤ RIEŠENIA ONELOGIN IAM MOŽNO ZNEUŽIŤ NA EXTRAKCIU TAJNÝCH HODNÔT OIDC

Spoločnosť One Identity vydala bezpečnostné aktualizácie svojho IAM (Identity and Access Management) riešenia OneLogin, ktoré opravujú zraniteľnosť vysokej závažnosti. CVE-2025-59363 umožňuje enumeráciu aplikácií a získanie tajných hodnôt OIDC (OpenID Connect). Tie možno následne zneužiť na získanie neoprávneného prístupu do systému. Viac informácií na stránke.

ZÁVAŽNÉ ZRANITEĽNOSTI VO VMWARE NSX A VCENTER UMOŽŇUJÚ ENUMERÁCIU POUŽÍVATEĽOV A INJEKCIU SMTP

Spoločnosť Broadcom vydala bezpečnostné aktualizácie VMware NSX a VMware vCenter, ktoré opravujú 3 vysoko závažné zraniteľnosti. Zraniteľnosti v NSX možno zneužiť na enumeráciu používateľov a následnú realizáciu brute-force alebo slovníkových útokov. Zraniteľnosť vo VMware vCenter umožňuje injektovať hlavičky SMTP. Viac informácií na stránke.

DRAYTEK OPRAVIL ZÁVAŽNÚ ZRANITEĽNOSŤ VO WEBOVOM ROZHRANÍ ROUTEROV VIGOR

Spoločnosť DrayTek vydala bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť viacerých routerov Vigor. CVE-2025-10547 možno zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V REDIS UMOŽŇUJE VZDIALENÉ VYKONANIE KÓDU

Vývojári in-memory NoSQL úložiska Redis vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú kritickú zraniteľnosť. CVE-2025-49844 by vzdialený autentifikovaný útočník mohol zneužiť na vykonanie kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V SIEŤOVÝCH ÚLOŽISKÁCH WD MY CLOUD UMOŽŇUJE VZDIALENÉ VYKONANIE KÓDU

Spoločnosť Western Digital vydala aktualizácie firmvéru viacerých modelov zariadení NAS (Network Attached Storage) série My Cloud, ktoré opravujú kritickú zraniteľnosť. CVE-2025-30247 možno zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

ZRANITEĽNOSŤ V ORACLE E-BUSINESS SUITE

Spoločnosť Oracle vydala bezpečnostnú aktualizáciu na svoj produkt E-Business Suite, ktorá opravuje vysoko závažnú zraniteľnosť. CVE-2025-61884 by vzdialený neautentifikovaný útočník zaslaním špeciálne vytvorených HTTP požiadaviek mohol zneužiť na kompromitáciu Oracle Configurator a získanie neoprávneného prístupu k citlivým údajom. Zraniteľnosť bola pridaná do zoznamu aktívne zneužívaných. Viac informácií na stránke.

JUNIPER NETWORKS VYDÁVA VEĽKÝ BALÍK BEZPEČNOSTNÝCH OPRÁV

Spoločnosť Juniper Networks opravila zhruba 220 zraniteľností vo svojich produktoch Junos OS, Junos Space a Junos Space Security Director. 9 z nich je kritických. Viac informácií na stránke.

ÚTOČNÍCI UKRADLI ZDROJOVÝ KÓD A POPISY ZRANITEĽNOSTÍ F5 BIG-IP, AKTUALIZUJTE IHNEĎ!

Spoločnosť F5 potvrdila, že sa stala obeťou kybernetického útoku, v rámci ktorého sa bližšie nešpecifikovanej štátom sponzorovanej skupine podarilo získať dlhodobý prístup do ich systémov a exfiltrovať citlivé údaje, vrátane zdrojového kódu a konfigurácií časti zákazníkov. Viac informácií na stránke.

AUTOMATICKÝ VYTÁČACÍ SYSTÉM ICTBROADCAST OBSAHUJE AKTÍVNE ZNEUŽÍVANÚ ZRANITEĽNOSŤ

Výskumníci z VulnCheck zverejnili informácie o aktívne zneužívanej kritickej zraniteľnosti v softvéri ICTBroadcast spoločnosti ICT Innovations, ktorý slúži na správu call centier a automatické vytáčanie hovorov. CVE-2025-2611 možno zneužiť na injekciu shellových príkazov a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

ZRANITEĽNOSŤ V UEFI MODULÁRNYCH POČÍTAČOV FRAMEWORK UMOŽŇUJE INŠTALÁCIU BOOTKITOV

Výrobca modulárnych notebookov a desktopov Framework vydal bezpečnostné aktualizácie firmvéru svojich produktov, ktoré opravujú zraniteľnosť zneužiteľnú na inštaláciu bootkitov a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

PROSTREDIA CURSOR A WINDSURF OBSAHUJÚ DESIATKY ZRANITEĽNOSTÍ

Bezpečnostní výskumníci spoločnosti Ox Security upozornili na prítomnosť veľkého množstva známych zraniteľností v aktuálnych verziách vývojových prostredí Cursor a Windsurf, z dôvodu implementácie starých verzií nástrojov Chromium a V8. Výskumníci varujú, že ignorovanie či neaktualizovanie takýchto chýb predstavuje vážnu bezpečnostnú hrozbu. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V BRÁNACH TP-LINK OMADA

Spoločnosť TP-Link vydala bezpečnostné aktualizácie svojich brán Omada, ktoré opravujú 4 zraniteľnosti, z čoho 2 sú označené ako kritické. Kritické zraniteľnosti s identifikátormi CVE-2025-6542 a CVE-2025-7850 možno zneužiť na vzdialené vykonanie príkazov operačného systému a získanie úplnej kontroly nad systémom. Viac informácií na stránke.