MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

FEBRUÁR 2025

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci február 2 kritické a 35 vysoko závažných zraniteľností v operačných systémoch Windows.

Komponent **Windows LDAP (Lightweight Directory Access Protocol)** obsahuje zraniteľnosť s identifikátorom CVE-2025-21376, ktorá spočíva v možnosti pretečenia vyrovnávacej pamäte a umožňuje **vzdialené vykonanie kódu**. Zraniteľnosť možno zneužiť bez autentifikácie, odoslaním špeciálne vytvorenej požiadavky na server LDAP, pričom pre úspešné zneužitie zraniteľnosti je potrebné, aby útočník vyhral súbeh procesov.

Zraniteľnosť s identifikátorom CVE-2025-21379 sa nachádza v službe **DHCP Client** a vzdialený neautentifikovaný útočník vy ju mohol zneužiť na **vzdialené vykonanie kódu**. Zneužitie zraniteľnosti vyžaduje prístup k rovnakému sieťovému segmentu. Útočník potrebuje zneužiť techniky Man-in-the-Middle.

Vysoko závažné zraniteľnosti vo **Windows Server 2016** (CVE-2025-21200, CVE-2025-21407, CVE-2025-21368, CVE-2025-21371, CVE-2025-21201, CVE-2025-21190, CVE-2025-21410, CVE-2025-21406, CVE-2025-21208, CVE-2025-21369) 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, obídenie bezpečnostných prvkov a realizáciu spoofing útokov.

Zraniteľné systémy:

- 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 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-2025-21376
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21379

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 február bezpečnostné aktualizácie, ktoré opravujú 2 kritické a 11 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritická zraniteľnosť v **Microsoft Bing** spočíva chýbajúcej autentifikácii pre dôležitú funkciu aplikácie (CVE-2025-21355). Neautentifikovaný útočník by ju mohol zneužiť na **vykonanie kódu** v rámci siete. Zraniteľnosť mitigovala spoločnosť Microsoft a nie sú potrebné ďalšie kroky pre jej odstránenie.

Microsoft Excel obsahuje kritickú zraniteľnosť s identifikátorom CVE-2025-21381, ktorú by neautentifikovaný útočník mohol zneužiť na **vykonanie ľubovoľného kódu**. Zraniteľnosť súvisí s dereferenciou nedôveryhodného ukazovateľa a jej zneužitie vyžaduje interakciu obete.

Vysoko závažné zraniteľnosti v produktoch **Microsoft Excel** (CVE-2025-21383, CVE-2025-21386, CVE-2025-21387 a CVE-2025-21390), **Microsoft Office 2016** (CVE-2025-21392), **Microsoft Office 2019** (CVE-2025-21394), **Microsoft Office LTSC 2024** (CVE-2025-21397), **Microsoft Outlook** (CVE-2025-21259), **Microsoft PC Manager** (CVE-2025-21322), **Microsoft AutoUpdate for Mac** (CVE-2025-24036) a **Microsoft SharePoint Server** (CVE-2025-21400) spočívajú v pretečení medzipamäte haldy, možnosti čítania pamäte mimo povolené hodnoty, použití odalokovaného miesta v pamäti, súbehu TOCTOU, nevhodnej autorizácii, nesprávnej reprezentácii kritickej informácie a nedostatočnou ochranou pred traverzovaním súborového systému pomocou odkazov. Predmetné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu, eskaláciu oprávnení, získanie citlivých informácií a falšovanie identity**.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft AutoUpdate for Mac
- Microsoft Bing
- 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 Outlook for Android
- Microsoft PC Manager
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription 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-2025-21355
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21381

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 február opravila 4 vysoko závažné zraniteľnosti vo webovom prehliadači Microsoft Edge.

Vysoko závažné zraniteľnosti s identifikátorom CVE-2025-21279, CVE-2025-21283, CVE-2025-21342 a CVE-2025-21408 spočívajú v absentujúcom overovaní typu premennej a v nedostatočnej granularite ochrany adresných oblastí pomocou uzamknutých registrov. Vzdialený neautentifikovaný útočník by ju mohol zneužiť na vzdialené vykonanie kódu. Zneužitie zraniteľností vyžaduje interakciu zo strany obete, ktorá musí kliknúť na špeciálne vytvorený URL odkaz.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft Edge (Chromium-based) 133.0.6943.53/54

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-2025-21279
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21283
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21342
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21408

MOZILLA FIREFOX

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

Bližšie nešpecifikované zraniteľnosti s označením CVE-2025-1016 (línie Firefox, Firefox ESR) a CVE-2025-1020 a CVE-2025-1414 (línia Firefox) možno zneužiť na **poškodenie obsahu pamäte** a **vzdialené vykonanie kódu**.

CVE-2025-1009 v komponente XSLT v línii Firefox umožňuje použiť dealokované miesto v pamäti a **spôsobiť pád systému**. Zraniteľnosť je možné zneužiť pomocou špeciálne vytvorených dát pre XSLT.

CVE-2025-1010 v komponente Custom Highlight v línii Firefox umožňuje použiť dealokované miesto v pamäti a **spôsobiť pád systému**. Zraniteľnosť je možné zneužiť pomocou špeciálne vytvorených dát pre Custom Highlight.

CVE-2025-27426 v línii Firefox pre iOS umožňuje presmerovať na falošnú webstránku. Zneužiť ju možno, pokiaľ škodlivá webstránka používa presmerovanie na chybovú stránku na strane servera.

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox verzie staršie ako 136
- Mozilla Firefox ESR verzie staršej ako 115.20 a 128.7

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 136 a Firefox ESR na verziu 115.20 alebo 128.7.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-07/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-08/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-09/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-12/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-13/

GOOGLE CHROME

V mesiaci február spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 8 vysoko závažných zraniteľností.

Zraniteľnosti v komponente **V8** spočívajú v možnosti použitia dealokovaného miesta v pamäti (CVE-2025-0445, CVE-2025-0995), prístupe k pamäti mimo povolených hodnôt (CVE-2025-0998) a pretečení medzipamäte na halde (CVE-2025-0999). Vzdialený neautentifikovaný útočník by ich mohol zneužiť napríklad na **vzdialené vykonanie kódu**.

Použitie dealokovaného miesta v pamäti v rámci komponentov **Skia** (CVE-2025-0444) a **Navigation** (CVE-2025-0997), nevhodnú implementáciu nešpecifikovaných funkcií v **Browser UI** (CVE-2025-0996) a pretečenie vyrovnávacej pamäte haldy v komponente **GPU** (CVE-2025-1426) možno zneužiť napríklad na **vzdialené vykonanie kódu** a **podhodenie falošného obsahu do URL baru**.

Zneužitie všetkých vyššie uvedených zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť špeciálne vytvorený webový obsah.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows a Mac verzie staršej ako 133.0.6943.141/.142
- Google Chrome pre Linux verzie staršej ako 133.0.6943.141

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 133.0.6943.141/.142 a Linux verzie aspoň na verziu 133.0.6943.141.

ZDROJE:

- https://chromereleases.googleblog.com/2025/02
- https://chromereleases.googleblog.com/2025/02/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2025/02/stable-channel-update-for-desktop_12.html
- https://chromereleases.googleblog.com/2025/02/stable-channel-update-for-desktop_18.html

- https://chromereleases.googleblog.com/2025/02/stable-channel-update-for-desktop_25.html
- https://nvd.nist.gov/vuln/detail/CVE-2025-0444
- https://nvd.nist.gov/vuln/detail/CVE-2025-0445
- https://nvd.nist.gov/vuln/detail/CVE-2025-0995
- https://nvd.nist.gov/vuln/detail/CVE-2025-0996
- https://nvd.nist.gov/vuln/detail/CVE-2025-0997
- https://nvd.nist.gov/vuln/detail/CVE-2025-0998
- https://nvd.nist.gov/vuln/detail/CVE-2025-0999
- https://nvd.nist.gov/vuln/detail/CVE-2025-1426

4. ADOBE ACROBAT A READER

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

Zraniteľnosť CVE-2025-24070 spočíva v slabých 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

ZERO-DAY ZRANITEĽNOSTI ADVANTIVE VERACORE

Advantive VeraCore obsahuje dve aktívne zneužívané zraniteľnosti, z ktorých jedna umožňuje nahrávanie súborov do ľubovoľného priečinku zraniteľnej aplikácie a druhá umožňuje získať kontrolu nad databázou. Útočníci zo skupiny XE Group zreťazujú tieto zraniteľnosti pre nasadenie webshellov. Viac informácií na stránke.

KRITICKÉ A AKTÍVNE ZNEUŽÍVANÉ ZERO-DAY ZRANITEĽNOSTI V PRODUKTOCH APPLE

Spoločnosť APPLE vydala bezpečnostné aktualizácie, ktoré opravujú 69 bezpečnostných zraniteľností v operačných systémoch iOS, iPadOS, macOS, tvOS, watchOS a visionOS a webovom prehliadači Safari, z čoho 18 je označených ako kritických a 1 ako aktívne zneužívaná zero-day zraniteľnosť. Aktívne zneužívanú zero-day s označením CVE-2025-24085 možno zneužiť na eskaláciu privilégií na zariadeniach s tvOS, watchOS, macOS Sequoia, iOS, iPadOS a visionOS. Viac informácií na stránke.

Spoločnosť Apple opravila aktívne zneužívanú zraniteľnosť CVE-2025-24200 v operačných systémoch iOS a iPadOS, ktorú by útočník s fyzickým prístupom k uzamknutým zariadeniam mohol zneužiť na deaktiváciu bezpečnostného mechanizmu USB Restricted Mode. Viac informácií na stránke.

VYSOKO ZÁVAŽNÉ ZRANITEĽNOSTI V DNS SYSTÉME BIND MOŽNO ZNEUŽIŤ NA ZNEPRÍSTUPNENIE SLUŽBY

Vývojári DNS systému BIND vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú dve vysoko závažné zraniteľnosti. CVE-2024-12705 a CVE-2024-11187 možno zneužiť na zahltenie dostupných prostriedkov a zneprístupnenie služby. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ MONITOROVACIEHO A MANAŽMENTOVÉHO FRAMEWORKU CACTI

Vývojári open-source monitorovacieho a manažmentového frameworku Cacti vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú dve zraniteľnosti, z čoho jedna je označená ako kritická. Kritickú zraniteľnosť s označením CVE-2025-22604 možno zneužiť na vzdialené vykonanie kódu. Viac informácií na stránke.

ZRANITEĽNOSTI V NÁSTROJOCH PLATFORMY GITHUB MOŽNO ZNEUŽIŤ NA ZÍSKANIE AUTENTIFIKAČNÝCH ÚDAJOV

Vývojári platformy GitHub vydali bezpečnostné aktualizácie svojich produktov GitHub Desktop, Git LFS, GitHub CLI/Codespaces a Git Credential Manager, ktoré opravujú 4 zraniteľnosti, z čoho 2 sú označené ako vysoko závažné. Zraniteľnosti súhrnne označené ako „Clone2Leak“ možno zneužiť na získanie neoprávneného prístupu k prihlasovacím údajom a autentifikačným tokenom. Viac informácií na stránke.

VYSOKO ZÁVAŽNÉ ZRANITEĽNOSTI V PHP BALÍKU VOYAGER POUŽÍVANÉHO NA SPRÁVU APLIKÁCIÍ LARAVEL

Bezpečnostní výskumníci zo spoločnosti SonarSource zverejnili informácie o 3 bezpečnostných zraniteľnostiach open-source PHP balíka Voyager používaného na správu Laravel aplikácií. Zreťazením zraniteľností CVE-2024-55417 a CVE-2024-55416 možno dosiahnuť vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

VYSOKO ZÁVAŽNÉ ZRANITEĽNOSTI V PRODUKTOCH VMWARE AVI LOAD BALANCER, ARIA OPERATIONS A CLOUD FOUNDATION

Spoločnosť Broadcom vydala bezpečnostné aktualizácie, ktoré opravujú 6 zraniteľností v produktoch VMware AVI Load Balancer, Aria Operations a Cloud Foundation, z ktorých 4 sú označené ako vysoko závažné. Najzávažnejšie zraniteľnosti možno zneužiť na získanie neoprávneného prístupu k databáze (CVE-2025-22217 – AVI Load Balancer) a k prihlasovacím údajom produktov VMware integrovaných do Aria Operations for Logs (CVE-2025-22218). Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÉ ZERO-DAY ZRANITEĽNOSTI V ZYXEL ZARIADENIACH SÉRIE CPE

Bezpečnostní výskumníci z Greynoise a Vulncheck varujú pred aktívnym zneužívaním kritických zero-day zraniteľností v zariadeniach Zyxel CPE. CVE-2024-40891 a CVE-2024-40891 možno zneužiť na vzdialené vykonanie príkazov a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

ÚTOČNÍCI AKTÍVNE ZNEUŽÍVAJÚ VEREJNE DOSTUPNÉ ASP.NET KĽÚČE NA VZDIALENÉ VYKONANIE KÓDU

Spoločnosť Microsoft varovala pred útokmi na aplikácie ASP.NET, v rámci ktorých útočníci na vzdialené vykonanie kódu a šírenie malvéru zneužívajú verejne dostupné statické strojové kľúče (machine keys) ASP.NET. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI ZIMBRA COLLABORATION

V produkte Zimbra Collaboration boli opravené dve kritické a jedna stredne závažná zraniteľnosť. Tieto umožňujú útočníkom získať metadáta e-mailov alebo presmerovanie na koncové body v rámci vnútornej siete. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ WAZUH UMOŽŇUJE VYKONÁVAŤ KÓD

Vývojári open-source SIEM a XDR platformy Wazuh vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú kritickú zraniteľnosť. Táto umožňuje vzdialene vykonávať kód Python. Na uvedenú zraniteľnosť je dostupný proof-of-concept kód demonštrujúci postup jej zneužitia. Viac informácií na stránke.

KRITICKÉ BEZPEČNOSTNÉ ZRANITEĽNOSTI V PRODUKTOCH ADOBE

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty InDesign, Commerce, Substance 3D Stager, InCopy, Illustrator, Substance 3D Designer a Photoshop Elements, ktoré opravujú 45 zraniteľností, z čoho 23 je označených ako kritických. Kritické zraniteľnosti by útočník mohol zneužiť na vykonanie škodlivého kódu, obídenie bezpečnostných prvkov a eskaláciu privilégií. Viac informácií na stránke.

KRITICKÉ BEZPEČNOSTNÉ ZRANITEĽNOSTI V CISCO IDENTITY SERVICES ENGINE

Spoločnosť Cisco vydala bezpečnostné aktualizácie pre svoj produkt Cisco Identity Services Engine a Cisco Identity Services Engine – Passive Identity Connector, ktoré opravujú 2 kritické zraniteľnosti. Zraniteľnosti s označením CVE-2025-20124 a CVE-2025-20125 možno zneužiť na vzdialené vykonanie príkazov, eskaláciu privilégií, vykonanie neoprávnených zmien v systéme a zneprístupnenie služby. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V PRODUKTOCH IVANTI ICS, IPS, ISAC A CSA

Spoločnosť Ivanti vydala bezpečnostné aktualizácie pre svoje produkty Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS), Ivanti Secure Access Client (Ivanti Secure Access Client) a Ivanti

Cloud Services Application (CSA), ktoré opravujú 10 zraniteľností, z čoho 4 sú označené ako kritické. Kritické zraniteľnosti umožňujú vzdialené vykonanie kódu, získanie neoprávneného prístupu k citlivým údajom a vykonanie neoprávnených zmien v systéme. Viac informácií na stránke.

Aktívne zneužívaná zraniteľnosť v operačnom systéme Palo Alto PAN-OS

Spoločnosť Palo Alto Networks vydala bezpečnostné aktualizácie pre svoj sieťový operačný systém PAN-OS, ktoré opravujú 4 zraniteľnosti, z ktorých 1 je označená ako aktívne zneužívaná. Zraniteľnosti nachádzajúce sa vo webovom manažmentovom rozhraní a plugine OpenConfig možno zneužiť na injekciu príkazov, získanie neoprávneného prístupu k citlivým údajom a vykonanie neoprávnených zmien v systéme. CVE-2025-0108 je podľa spoločnosti GreyNoise v súčasnosti aktívne zneužívaná útočníkmi. Viac informácií na stránke.

Aktívne zneužívaná zraniteľnosť v databázovom systéme PostgreSQL

Vývojári databázového systému PostgreSQL vydali bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú zero-day zraniteľnosť vysokej závažnosti. CVE-2025-1094 vo viacerých funkciách libpq možno zneužiť na vzdialené vykonanie kódu. Viac informácií na stránke.

Kritická zraniteľnosť v distribuovanej databáze Apache Ignite

Vývojári distribuovanej databázy Apache Ignite vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú kritickú zraniteľnosť. CVE-2024-52577 by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu. Viac informácií na stránke.

Závažná zraniteľnosť Citrix NetScaler Console a Agent

Spoločnosť Citrix vydala bezpečnostné aktualizácie pre svoje produkty NetScaler Console a NetScaler Agent, ktoré opravujú vysoko závažnú zraniteľnosť. Táto umožňuje autentifikovanému útočníkovi eskalovať svoje privilégiá a vzdialene vykonávať príkazy. Viac informácií na stránke.

Závažné zraniteľnosti OpenSSH

Vývojári OpenSSH vydali bezpečnostné aktualizácie, ktoré opravujú dve zraniteľnosti umožňujúce realizáciu útokov typu man-in-the-middle a zneprístupnenie služby. Úspešným zneužitím zraniteľností môže útočník získať prístup k citlivým informáciám a prevziať kontrolu nad SSH reláciou. Viac informácií na stránke.

ATLASSIAN OPRAVUJE KRITICKÉ ZRANITEĽNOSTI VIACERÝCH PRODUKTOV

Spoločnosť Atlassian vydala bezpečnostné aktualizácie na svoje produkty Confluence, Bamboo, Bitbucket, Crowd a Jira, ktoré opravujú 7 zraniteľností, z čoho 3 sú označené ako kritické. Kritické zraniteľnosti v Confluence a Crowd je možné zneužiť na vzdialené vykonanie kódu a obídenie mechanizmov autentifikácie. Ostatné zraniteľnosti je možné zneužiť na zneprístupnenie služby. Viac informácií na stránke.