# MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

JANUÁR 2025

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

## 1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci január 8 kritických a 135 vysoko závažných zraniteľností v operačných systémoch Windows.

Komponent **Microsoft Digest Authentication** obsahuje zraniteľnosť s identifikátorom CVE-2025-21294, ktorá spočíva v ukladaní citlivých údajov v nesprávne uzamknutej pamäti a umožňuje **vzdialené vykonanie kódu**. Zraniteľnosť možno zneužiť pripojením sa na systémy využívajúce autentifikáciu prostredníctvom Digest Authentication, pričom pre úspešné zneužitie zraniteľnosti je potrebné, aby útočník vyhral súbeh procesov.

Zraniteľnosť s identifikátorom CVE-2025-21295 sa nachádza v bezpečnostnom mechanizme **SPNEGO Extended Negotiation (NEGOEX)** a vzdialený neautentifikovaný útočník vy ju mohol zneužiť na **vzdialené vykonanie kódu**. Zneužitie zraniteľnosti nevyžaduje interakciu zo strany používateľa.

Zraniteľnosť v komponente **BranchCache** by neautentifikovaný útočník nachádzajúci sa v rovnakom sieťovom segmente mohol zneužiť na **vykonanie kódu**. CVE-2025-21296 spočíva v použití odalokovaného miesta v pamäti. Úspešné zneužitie zraniteľnosti vyžaduje, aby útočník vyhral súbeh procesov.

Komponent **Windows Remote Desktop Services** obsahuje dve kritické zraniteľnosti, ktoré možno zneužiť na **vzdialené vykonanie kódu**. Prvá zraniteľnosť s označením CVE-2025-21297 spočíva v použití odalokovaného miesta v pamäti. CVE-2025-21309 spočíva v ukladaní citlivých dát v nesprávne uzamknutej pamäti. Zraniteľnosti možno zneužiť pripojením sa na zraniteľné systémy v konfigurácii Remote Desktop Gateway. Úspešné zneužitie zraniteľností vyžaduje, aby útočník vyhral súbeh procesov.

Kritickú zraniteľnosť CVE-2025-21298 v komponente **Windows OLE (Object Linking and Embeding)** využívanom v rámci e-mailového klienta **Microsoft Outlook** by vzdialený neautentifikovaný útočník zaslaním špeciálne vytvorených e-mailov mohol zneužiť na **vzdialené vykonanie kódu**. Úspešné zneužitie zraniteľnosti vyžaduje zobrazenie náhľadu alebo otvorenie špeciálne vytvorenej e-mailovej správy. **Spoločnosť Microsoft odporúča nastaviť Microsoft Outlook, aby e-mailové správy zobrazoval v plaintextovom režime**, v rámci ktorého nedochádza

k zobrazeniu obrázkov, špecializovaných fontov, animácií a ďalšieho zneužiteľného obsahu. Kompletný návod môžete nájsť na stránke výrobcu.

Použitie odalokovaného miesta v pamäti v rámci ovládača **Windows RMCAST (Reliable Multicast Transport)** možno zaslaním špeciálne vytvorených paketov na otvorené PGM (Pragmatic General Multicast) sockety zneužiť na **vzdialené vykonanie kódu**. Zraniteľnosť s identifikátorom CVE-2025-21307 je možné zneužiť len na systémoch, na ktorých je prítomný program počúvajúci na PGM porte. Vzhľadom na to, že PGM nevykonáva autentifikáciu prichádzajúcich požiadaviek, spoločnosť **Microsoft odporúča PGM porty neprevádzkovať voľne dostupné z internetu a prístup k nim limitovať prostredníctvom sieťových a bezpečnostných prvkov.**

Komponent **Windows NTLM V1** obsahuje kritickú zraniteľnosť (CVE-2025-21311), ktorá spočíva v nesprávnej implementácii mechanizmov autentifikácie. Vzdialený neautentifikovaný útočník by ju mohol zneužiť na **eskaláciu privilégií** a **úplné narušenie dôvernosti, integrity a dostupnosti systému**. **Zraniteľnosť je možné mitigovať nastavením LmCompatibilityLvl na hodnotu 5** (maximálna možná hodnota), čo na systémoch znemožní využitie starého protokolu NTLMv1. Bližšie informácie môžete nájsť na stránke výrobcu.

**Vysoko závažné zraniteľnosti** v komponentoch **Windows Telephony Service** (CVE-2025-21417, CVE-2025-21413, CVE-2025-21411, CVE-2025-21409, CVE-2025-21339, CVE-2025-21306, CVE-2025-21305, CVE-2025-21303, CVE-2025-21302, CVE-2025-21286, CVE-2025-21282, CVE-2025-21273, CVE-2025-21266, CVE-2025-21252, CVE-2025-21250, CVE-2025-21248, CVE-2025-21246, CVE-2025-21245, CVE-2025-21244, CVE-2025-21243, CVE-2025-21241, CVE-2025-21240, CVE-2025-21239, CVE-2025-21238, CVE-2025-21237, CVE-2025-21236, CVE-2025-21233, CVE-2025-21223), **GDI+** (CVE-2025-21338), **Internet Explorer** (CVE-2025-21326), **Windows Direct Show** (CVE-2025-21291) a **Windows Line Printer Daemon (LPD) Service** (CVE-2025-21224) by vzdialený útočník mohol zneužiť na **vzdialené vykonanie kódu** a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Ostatné zraniteľnosti vysokej závažnosti možno zneužiť na vzdialené vykonanie kódu, eskaláciu privilégií, zneprístupnenie služby, získanie neoprávneného prístupu k citlivým údajom, obídenie bezpečnostných prvkov a realizáciu spoofing útokov.

## ZRANITEĽNÉ SYSTÉMY:

- 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 10 for 32-bit Systems
- Windows 10 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-2025-21294
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21295
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21296
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21297

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21298
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21307
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21309
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21311

## 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 január bezpečnostné aktualizácie, ktoré opravujú 3 kritické a 17 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritické zraniteľnosti v **Microsoft Excel** spočívajú v dereferencii nedôveryhodného ukazovateľa (CVE-2025-21354) a použití odalokovaného miesta v pamäti (CVE-2025-21362). Lokálny neautentifikovaný útočník by ich mohol zneužiť na **vykonanie kódu**.

**Microsoft Purview** obsahuje kritickú zraniteľnosť s identifikátorom CVE-2025-21385, ktorú by vzdialený autentifikovaný útočník mohol zneužiť na realizáciu **SSRF (Server Side Request Forgery) útokov** a následné **získanie neoprávneného prístupu k citlivým údajom**. Zraniteľnosť bola automaticky opravená spoločnosťou Microsoft a nevyžaduje dodatočnú aktualizáciu systémov.

Vysoko závažné zraniteľnosti v produktoch **Microsoft Access** (CVE-2025-21395, CVE-2025-21186, CVE-2025-21366), **Microsoft Office OneNote** (CVE-2025-21402), **Microsoft Office** (CVE-2025-21365), **Microsoft Word** (CVE-2025-21363), **Microsoft Outlook** (CVE-2025-21361, CVE-2025-21357), **Microsoft Office Visio** (CVE-2025-21356, CVE-2025-21345) spočívajú v pretečení medzipamäte haldy, použití odalokovaného miesta v pamäti, nesprávnych obmedzeniach pre názvy súborov a ostatných zdrojov, nedostatočnom overovaní vyhľadávacích ciest, dereferencii nedôveryhodného ukazovateľa, využití neinicializovaných prostriedkov a nesprávnom rozlišovaní dátových typov. Predmetné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu** s následkom **úplného narušenia dôvernosti, integrity a dostupnosti systému**. **Zneužitie zraniteľností vyžaduje interakciu zo strany obete, ktorá musí stiahnuť a otvoriť špeciálne vytvorené súbory.** Zraniteľnosť CVE-2025-21361 je možné zneužiť len na Outlook for Mac s ukončenou podporou.

**Microsoft SharePoint Server** obsahuje dve vysoko závažné zraniteľnosti, ktoré možno zneužiť na **vzdialené vykonanie kódu**. CVE-2025-21348 spočíva v nesprávnej autorizácii a umožňuje vzdialenému autentifikovanému útočníkovi s oprávneniami úrovne „Site Owner“ alebo vyššej vykonať škodlivý kód v kontexte SharePoint servera. Zraniteľnosť je možné zneužiť nahraním špeciálne vytvoreného súboru a následným zaslaním špeciálne vytvorenej API požiadavky, ktorá vedie k deserializácii parametrov tohto súboru. Zneužitie druhej zraniteľnosti s označením CVE-2025-21344 vyžaduje interakciu zo strany obete, ktorá musí otvoriť špeciálne vytvorené súbory.

## 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 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 Office for Android
- Microsoft Office for Mac
- Microsoft Office for Universal
- Microsoft Office for iOS
- Microsoft OneNote for Mac
- Microsoft Outlook 2016 (32-bit edition)
- Microsoft Outlook 2016 (64-bit edition)
- Microsoft Outlook for Mac
- Microsoft Purview
- 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-2025-21354
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21362
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21385

## 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 január opravila 1 vysoko závažnú zraniteľnosť vo webovom prehliadači Microsoft Edge.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2025-21185 spočíva v nedostatočnej implementácii mechanizmov riadenia prístupu a vzdialený neautentifikovaný útočník by ju mohol zneužiť na eskaláciu privilégií a získanie neoprávneného prístupu k citlivým údajom v API. Zneužitie zraniteľnosti vyžaduje interakciu zo strany obete, ktorá musí kliknúť na špeciálne vytvorený URL odkaz.

### ZRANITEĽNÉ SYSTÉMY:

- Microsoft Edge (Chromium-based) 134 132.0.6834.83/84

### 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-2025-21185

## MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci január opravila 3 vysoko závažné zraniteľnosti v línii internetových prehliadačov Firefox a Firefox ESR. Bližšie nešpecifikované zraniteľnosti s označením CVE-2025-0242 (línie Firefox, Firefox ESR) a CVE-2025-0247 (línia Firefox) možno zneužiť na **poškodenie obsahu pamäte** a **vzdialené vykonanie kódu**.

CVE-2025-0244 v línii Firefox možno presmerovaním na neplatnú protokolovú schému zneužiť na **spoofing lišty pre zadávanie adries**. Zraniteľnosť je možné zneužiť len na zariadeniach s operačným systémom Android.

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

### ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox verzie staršie ako 134
- Mozilla Firefox ESR verzie staršej ako 128.6

### ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 134 a Firefox ESR na verziu 128.6.

### ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-03/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-02/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-01/

## GOOGLE CHROME

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

Zraniteľnosti v komponente V8 spočívajú v nesprávnom overovaní dátových typov (CVE-2025-0291), čítaní pamäte mimo povolených hodnôt (CVE-2025-0434, CVE-2025-0612) a poškodení objektov (CVE-2025-0611). Vzdialený neautentifikovaný útočník by ich mohol zneužiť na vzdialené vykonanie kódu.

CVE-2025-0435 v komponente Navigation možno zneužiť na realizáciu útokov kategórie spoofing modifikujúcich používateľské rozhranie.

Pretečenie celočíselnej premennej v rámci komponentu Skia (CVE-2025-0436), pretečenie vyrovnávacej pamäte zásobníka v komponente Tracing (CVE-2025-0438) a čítanie pamäte mimo povolených hodnôt v komponente Metrics (CVE-2025-0437) možno zneužiť na vzdialené vykonanie kódu.

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 132.0.6834.159/160
- Google Chrome pre Linux verzie staršej ako 132.0.6834.159

### ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 131.0.6778.85/.86 a Linux verzie aspoň na verziu 131.0.6778.85.

### ZDROJE:

- https://chromereleases.googleblog.com/2025
- https://chromereleases.googleblog.com/2025/01/stable-channel-update-for-desktop_28.html
- https://chromereleases.googleblog.com/2025/01/stable-channel-update-for-desktop_22.html
- https://chromereleases.googleblog.com/2025/01/stable-channel-update-for-desktop_14.html
- https://chromereleases.googleblog.com/2025/01/stable-channel-update-for-desktop.html
- https://nvd.nist.gov/vuln/detail/CVE-2025-0291
- https://nvd.nist.gov/vuln/detail/CVE-2025-0434
- https://nvd.nist.gov/vuln/detail/CVE-2025-0611
- https://nvd.nist.gov/vuln/detail/CVE-2025-0612
- https://nvd.nist.gov/vuln/detail/CVE-2025-0435
- https://nvd.nist.gov/vuln/detail/CVE-2025-0436
- https://nvd.nist.gov/vuln/detail/CVE-2025-0437
- https://nvd.nist.gov/vuln/detail/CVE-2025-0438

## 4. ADOBE ACROBAT A READER

V mesiaci január 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 január spoločnosť Microsoft opravila 4 vysoko závažné zraniteľnosti vo frameworku .NET.

Zraniteľnosti spočívajúce v pretečení medzipamäte haldy a vytváraní dočasných súborov v nedostatočne zabezpečených priečinkoch možno zneužiť na **vzdialené vykonanie kódu** (CVE-

2025-21171) a **eskaláciu privilégií** (CVE-2025-21173). **Zneužitie zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí v aplikácii .NET spustiť škodlivý payload.**

CVE-2025-21172 spočíva v pretečení celočíselnej premennej a pretečení medzipamäte haldy a zraniteľnosť s identifikátorom CVE-2025-21176 spočíva v nesprávnom čítaní zásobníka. Obe zraniteľnosti možno zneužiť na **vzdialené vykonanie kódu**. **Zneužitie zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť špeciálne vytvorený balík v aplikácii Visual Studio.**

## ZRANITEĽNÉ SYSTÉMY:

- .NET 8.0 installed on Linux
- .NET 8.0 installed on Mac OS
- .NET 8.0 installed on Windows
- .NET 9.0 installed on Linux
- .NET 9.0 installed on Mac OS
- .NET 9.0 installed on Windows
- Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2
- Microsoft .NET Framework 3.5 AND 4.7.2
- Microsoft .NET Framework 3.5 AND 4.8
- Microsoft .NET Framework 3.5 AND 4.8.1
- Microsoft .NET Framework 4.6.2
- Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2
- Microsoft .NET Framework 4.6/4.6.2
- Microsoft .NET Framework 4.8
- Microsoft Visual Studio 2017 version 15.9
- Microsoft Visual Studio 2022 version 17.12
- Microsoft Visual Studio 2022 version 17.10
- Microsoft Visual Studio 2022 version 17.8
- Microsoft Visual Studio 2022 version 17.6
- Microsoft Visual Studio 2019 version 16.11

### 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-2025-21171
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21172
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21173
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21176

## ORACLE JAVA

Spoločnosť Oracle v mesiaci január vydala bezpečnostné aktualizácie, ktoré opravujú 1 vysoko závažnú zraniteľnosť v rámci Oracle Java SE.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2025-0509 sa nachádza v komponente Install (Sparkle) a autentifikovaný útočník nachádzajúci sa v rovnakom sieťovom segmente by ju mohol zneužiť na získanie úplnej kontroly nad zraniteľnou inštanciou Oracle Java SE.

### ZRANITEĽNÉ SYSTÉMY:

- Oracle Java SE: 8u431

### 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/cpujan2025.html
- https://www.oracle.com/security-alerts/cpujan2025verbose.html#JAVA

# 6. INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

## AKTÍVNE ZNEUŽÍVANÁ KRITICKÁ ZERO-DAY ZRANITEĽNOSŤ V ZARIADENIACH SONICWALL SECURE MOBILE ACCESS 1000

Spoločnosť SonicWall vydala bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú kritickú zero-day zraniteľnosť v zariadeniach SonicWall Secure Mobile Access série 1000. CVE-2025-23006 možno zneužiť na vzdialené vykonanie systémových príkazov a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

## ZRANITEĽNOSTI V PRODUKTOCH CISCO MEETING MANAGEMENT, SECURE ENDPOINT CONNECTOR A BROADWORKS

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje produkty Meeting Management, Secure Endpoint Connector (Linux, Mac a Windows verzie), Secure Endpoint Private Cloud a BroadWorks, ktoré opravujú viaceré zraniteľnosti. Kritickú zraniteľnosť CVE-2025-20156 v Cisco Meeting Management možno zneužiť na eskaláciu privilégií a získanie úplnej kontroly nad systémom. Ostatné zraniteľnosti umožňujú zneprístupnenie služby. Viac informácií na stránke.

## ZRANITEĽNOSŤ V 7-ZIP UMOŽŇUJE OBÍDENIE OCHRANY MARK-OF-THE-WEB A VYKONANIE ŠKODLIVÉHO KÓDU

Vývojári komprimačného nástroja 7-Zip vydali bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť. CVE-2025-0411 možno podvrhnutím špeciálne vytvorených súborov zneužiť na obídenie bezpečnostného mechanizmu „Mark of the Web“ a vzdialené vykonanie kódu. Viac informácií na stránke.

## KRITICKÉ ZRANITEĽNOSTI VO WORDPRESS PLUGINOCH REALHOMES THEME A EASY REAL ESTATE

Bezpečnostní výskumníci zo spoločnosti Patchstack zverejnili informácie o kritických zraniteľnostiach vo WordPress pluginoch RealHomes Theme a Easy Real Estate, ktoré možno zneužiť na eskaláciu privilégií, získanie administrátorského prístupu a úplnej kontroly nad systémom. Viac informácií na stránke.

## KRITICKÁ ZRANITEĽNOSŤ V NÁSTROJI PRE PRENOS A SYNCHRONIZÁCIU SÚBOROV RSYNC

Vývojári open source nástroja pre prenos a synchronizáciu súborov RSYNC vydali bezpečnostné aktualizácie, ktoré opravujú 6 zraniteľností, z čoho 1 je označená ako kritická. CVE-2024-12084 možno zneužiť na vzdialené vykonanie kódu. Zreťazením zraniteľností CVE-2024-12084 a CVE-2024-12085 možno získať úplnú kontrolu nad zraniteľnými systémami. Viac informácií na stránke.

## KRITICKÉ ZRANITEĽNOSTI V NÁSTROJI PRE VZDIALENÝ PRÍSTUP SIMPLEHELP

Vývojári riešenia pre vzdialený prístup SimpleHelp vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú 3 kritické zraniteľnosti. Kombináciou uvedených zraniteľností možno získať úplnú kontrolu nad zraniteľnými systémami. Zraniteľnosti sú aktívne zneužívané útočníkmi. Viac informácií na stránke.

## KRITICKÉ ZRANITEĽNOSTI VO WEBOVÝCH APLIKAČNÝCH SERVEROCH SAP NETWEAVER

Spoločnosť SAP vydala bezpečnostné aktualizácie svojho webového aplikačného servera NetWeaver, ktoré opravujú 8 zraniteľností, z čoho 2 sú označené ako kritické. CVE-2025-0070 a CVE-2025-0066 možno zneužiť na eskaláciu privilégií a získanie neoprávneného prístupu k citlivým údajom. Viac informácií na stránke.

## MICROSOFT V JANUÁROVOM PATCH TUESDAY OPRAVIL 12 KRITICKÝCH ZRANITEĽNOSTÍ

Spoločnosť Microsoft vydala v januári 2025 balík opráv pre portfólio svojich produktov opravujúci 161 zraniteľností, z ktorých 58 umožňuje vzdialené vykonanie kódu. Kritické zraniteľnosti sa nachádzajú v Microsoft Digest Authentication, NEGOEX, BranchCache, Windows Remote Desktop Services, Windows OLE, Windows RMCAST, Windows NTLM V1, Azure Marketplace SaaS Resources, Microsoft Purview a Microsoft Excel a možno ich zneužiť vzdialené vykonanie škodlivého kódu, eskaláciu privilégií a získanie neoprávneného prístupu k citlivým údajom. Windows Hyper-V NT Kernel Integration VSP obsahuje aktívne zneužívané zraniteľnosti umožňujúce eskaláciu privilégií (CVE-2025-21333, CVE-2025-21334, CVE-2025-21335). Viac informácií na stránke.

## KRITICKÉ ZRANITEĽNOSTI V PRODUKTOCH IVANTI ENDPOINT MANAGER, AVALANCHE, APPLICATION CONTROL ENGINE

Spoločnosť Ivanti vydala bezpečnostné aktualizácie pre svoje produkty Endpoint Manager (EPM), Avalanche, Application Control Engine, ktoré opravujú 20 zraniteľností, z ktorých 4 sú označené ako kritické. Kritické zraniteľnosti s označením CVE-2024-10811, CVE-2024-13161, CVE-2024-13160 a CVE-2024-13159 sa nachádzajú v produkte EPM a vzdialený neautentifikovaný útočník by ich mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom. Viac informácií na stránke.

## KRITICKÉ BEZPEČNOSTNÉ ZRANITEĽNOSTI V PRODUKTOCH ADOBE

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty Adobe Photoshop, Adobe Substance3D Stager, Adobe Illustrator for iPad, Adobe Animate, Adobe Substance3D Designer, ktoré opravujú 14 kritických zraniteľností. Uvedené zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vykonanie škodlivého kódu. Viac informácií na stránke.

## BEZPEČNOSTNÉ ZRANITEĽNOSTI V MIGRAČNOM NÁSTROJI PALO ALTO NETWORKS EXPEDITION

Spoločnosť Palo Alto Networks vydala bezpečnostné aktualizácie, ktoré opravujú 5 zraniteľností v migračnom nástroji Expedition. Najzávažnejšiu zraniteľnosť CVE-2025-0103 možno zneužiť na získanie neoprávneného prístupu k citlivým údajom a vytvorenie alebo odstránenie súborov na systémoch spravovaných prostredníctvom Expedition. Viac informácií na stránke.

## AKTÍVNE ZNEUŽÍVANÁ KRITICKÁ ZRANITEĽNOSŤ VO FIREWALLOCH FORTIGATE OD SPOLOČNOSTI FORTINET

Spoločnosť Fortinet vydala bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú kritickú zero-day zraniteľnosť v operačnom systéme FortiOS a produkte FortiProxy. CVE-2024-55591 možno zaslaním špeciálne vytvorenej požiadavky zneužiť na získanie administrátorského prístupu k zariadeniu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

## AKTÍVNE ZNEUŽÍVANÁ KRITICKÁ ZRANITEĽNOSŤ V PRODUKTE GFI KERIOCONTROL

Spoločnosť GFI vydala bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú kritickú zraniteľnosť v produkte KerioControl. CVE-2024-52875 možno zneužiť na vzdialené vykonanie kódu a následné získanie úplnej kontroly nad systémom. Viac informácií na stránke.

## KRITICKÉ ZRANITEĽNOSTI VO WORDPRESS PLUGINE FANCY PRODUCT DESIGNER

Bezpečnostní výskumníci zverejnili informácie o dvoch kritických zraniteľnostiach vo WordPress plugine Fancy Product Designer. Zraniteľnosti možno zneužiť na upload škodlivých súborov, vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

## VYSOKO ZÁVAŽNÉ ZRANITEĽNOSTI VO FIREWALLOCH SONICWALL S OPERAČNÝM SYSTÉMOM SONICOS

Spoločnosť SonicWall vydala bezpečnostné aktualizácie pre svoje firewally s operačným systémom SonicOS, ktoré opravujú 4 vysoko závažné zraniteľnosti. Najzávažnejšiu zraniteľnosť s označením CVE-2024-53704 možno zneužiť na obídenie mechanizmov autentifikácie a získanie neoprávneného prístupu do systému. Ostatné zraniteľnosti možno zneužiť na obídenie mechanizmov autentifikácie, realizáciu SSRF útokov a eskaláciu privilégií. Viac informácií na stránke.

## ZRANITEĽNOSTI ROUTEROV A SIEŤOVÝCH ZARIADENÍ MOXA

Spoločnosť Moxa vydala bezpečnostné aktualizácie svojich priemyselných routerov a sieťového príslušenstva, ktoré opravujú dve zraniteľnosti, z ktorých jedna je označená ako kritická. CVE-2024-9140 by vzdialený útočník mohol zneužiť na injekciu príkazov a vzdialené vykonanie škodlivého kódu a CVE-2024-9138 by útočník mohol zneužiť na eskaláciu privilégií na úroveň používateľa root. Viac informácií na stránke.

## ZRANITEĽNOSŤ KNIŽNICE PYTHON LIBARCHIVE UMOŽŇUJE DIRECTORY TRAVERSAL

Bezpečnostní analytici CSIRT.SK objavili zraniteľnosť v Python knižnici libarchive, ktorá umožňuje vykonávať útoky typu directory traversal. Zraniteľnosť je možné zneužiť na vykonanie neoprávnených zmien v systéme. V prípade prepísanie kritických súčastí operačného systému, ako sú napr. súbor authorized_keys obsahujúci SSH kľúče, vzniká aj riziko získania úplnej kontroly nad systémom. Viac informácií na stránke.