MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

JANUÁR 2026

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci január 3 kritické a 88 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritická zraniteľnosť CVE-2026-20822 v súčasti Microsoft Graphics Component súvisí s použitím dealokovaného miesta v pamäti. Lokálny útočník s nízkymi oprávneniami ju môže zneužiť na **navýšenie svojich oprávnení** až na úroveň **SYSTEM**. Na to musí vyhrať súbeh procesov.

Windows Local Security Authority Subsystem Service (LSASS) obsahuje kritickú zraniteľnosť CVE-2026-20854. Zraniteľnosť súvisí s použitím dealokovaného miesta v pamäti a útočníkovi s nízkymi oprávneniami umožňuje **vzdialene vykonávať kód**. Potrebuje na to modifikovať nešpecifikované atribúty priečinkov.

Tretiu opravenú kritickú zraniteľnosť CVE-2026-20876 vo Windows Virtualization-Based Security (VBS) Enclave spôsobuje neošetrené pretečenie pamäte na halde. Lokálny útočník s nízkymi oprávneniami ju môže zneužiť na **navýšenie svojich oprávnení** na úroveň Virtual Trust Level 2 (VTL2).

Vysoko závažné zraniteľnosti CVE-2026-0386, CVE-2026-20837, CVE-2026-20840, CVE-2026-20856, CVE-2026-20868 a CVE-2026-20922 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, odchádzanie bezpečnostných prvkov a spoofingové útoky.

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 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 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-2026-20822
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20854
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20876

Koniec podpory pre Windows 10, staršie verzie Windows 11 a Windows Server 2016

Spoločnosť Microsoft v roku 2025 plánovane ukončila podporu pre všetky verzie Windows 10. Po dátume 14. októbra 2025 už tieto produkty nedostávajú 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 predĺžila spoločnosť Microsoft 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:

23H2 Home a Pro: Podpora **skončila** 11. decembra 2025.
23H2 Enterprise a Education: Podpora skončí 10. decembra 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. 25H2.

2. KANCELÁRSKE BALÍKY MICROSOFT OFFICE A OFFICE WEB APPS

Spoločnosť Microsoft vydala v mesiaci január bezpečnostné aktualizácie, ktoré opravujú 8 kritických a 12 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritickú zraniteľnosť **Microsoft Word** s označením CVE-2026-20944 môže neautorizovaný lokálny útočník zneužiť na **vykonanie ľubovoľného škodlivého kódu**. Na to potrebuje poslať obeti škodlivý súbor MS Office. Chyba zabezpečenia súvisí s možnosťou čítania pamäte mimo povolené hodnoty. Útočným vektorom môže byť aj náhľad dokumentu (Preview Pane).

Kritické zraniteľnosti CVE-2026-20952 a CVE-2026-20953 v produkte **Microsoft Office** môže neautorizovaný útočník zneužiť na lokálne **vykonanie ľubovoľného škodlivého kódu**. Zraniteľnosti spočívajú v možnosti použitia dealokovaného miesta v pamäti. Zneužiť ich možno zaslaním škodlivého odkazu alebo súboru obeti, ktorá môže, no v niektorých prípadoch nemusí, ho otvoriť. Útočným vektorom môže byť aj náhľad dokumentu (Preview Pane).

Kritické zraniteľnosti **Microsoft Excel** s označením CVE-2026-20955 a CVE-2026-20957 môže neautorizovaný útočník zneužiť na lokálne **vykonanie škodlivého kódu**. Na to potrebuje poslať obeti škodlivý súbor MS Office. Chyby zabezpečenia súvisia s dereferencovaním nedôveryhodného ukazovateľa a pretečením vyrovnávacej pamäte na halde / podtečením celočíselnej premennej.

Kritická zraniteľnosť **Copilot Studio** s označením CVE- 2026-21520 súvisí s nedostatočnou kontrolou používateľských vstupov. Vzdialený neautentifikovaný útočník ju môže zneužiť na injektovanie príkazov a **získanie citlivých informácií**. Spoločnosť Microsoft zraniteľnosť opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre jej odstránenie.

Podobné zraniteľnosti sa nachádzajú v produkte **Word Copilot** (CVE-2026-21521) a **M365 Copilot** (CVE-2026-24307). Súvisí s nevhodnou sanitizáciou špeciálnych sekvencií a kontrolou používateľských vstupov. Vzdialený neautorizovaný útočník ju môže zneužiť **získanie citlivých informácií**. Spoločnosť Microsoft zraniteľnosti opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre jej odstránenie.

Vysoko závažné zraniteľnosti spočívajú v dereferencii nedôveryhodného ukazovateľa, deserializácii nedôveryhodných dát, možnosti čítania pamäte mimo povolené hodnoty, použití dealokovaného miesta v pamäti, neošetrení používateľských vstupov a vyhľadávacích ciest, možnosti vykonávať útoky typu SSRF a nevhodnej kontrole prístupov. Predmetné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu, získavanie citlivých informácií, obchádzanie bezpečnostných prvkov** a **útoky typu spoofing**.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft 365 Copilot
- Microsoft 365 Word Copilot
- Microsoft Copilot Studio
- 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 Deployment Tool
- 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 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-2026-20944
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20952
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20953
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20955
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20957
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21520
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21521

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-24307

Koniec podpory pre Office 2016 a Office 2019

Spoločnosť Microsoft v roku 2025 plánovane ukončila podporu pre Office 2016 a Office 2019. Po dátume 14. decembra 2025 už tieto produkty nedostávajú 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 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 január opravila 8 vysoko závažných zraniteľností v línii internetových prehliadačov Firefox a Firefox ESR.

Zraniteľnosť CVE-2026-0877 v komponente DOM: Security línií Firefox a Firefox ESR súvisí s možnosťou obísť nešpecifikovanú mitigáciu.

Zraniteľnosti CVE-2026-0878 a CVE-2026-0879 v línii Firefox a Firefox ESR v komponente Graphics: CanvasWebGL a Graphics vznikajú kvôli nesprávne nastaveným limitným podmienkam. Útočníkovi umožňujú uniknúť zo sandboxu.

Únik zo sandboxu umožňujú aj vysoko závažné zraniteľnosti CVE-2026-0880 v líniách Firefox a Firefox ESR a CVE-2026-0881 v línii Firefox. Prvá súvisí s pretečením celočíselnej premennej v komponente Graphics, druhá sa nachádza v komponente Messaging System.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť CVE-2026-0882 umožňujúcu použitie dealokovaného miesta v pamäti, ktorá sa nachádza v komponente IPC.

Línia Firefox obsahuje tiež zraniteľnosť CVE-2026-24869, ktorá vyplýva z možnosti použitia dealokovanej pamäte. Nachádza sa v komponente Layout: Scrolling and Overflow.

Identifikátor CVE-2026-0891 v línii Firefox a Firefox ESR opisuje sadu chýb pri narábaní s pamäťou. Táto zraniteľnosť ovplyvňuje bezpečnosť pamäte a môže viesť ku **poškodeniu pamäte** alebo možnosti **vykonávať kód**.

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox verzie staršie ako 147.0.2
- Mozilla Firefox ESR verzie staršej ako 115.32 a 140.7

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 147.0.2 a Firefox ESR na verziu 115.32 alebo 140.7.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-01/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-02/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-03/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-06/

GOOGLE CHROME

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

Komponent **V8** obsahuje tri vysoko závažné zraniteľnosti. CVE-2026-0899 súvisí s možnosťou prístupu k pamäti mimo povolené hodnoty, CVE-2026-0900 s nevhodnou implementáciou nešpecifikovaných prvkov a CVE-2026-1220 súvisí so súbehom procesov.

Vysoko závažná zraniteľnosť CVE-2026-0628 v komponente **WebView** súvisí s nedostatočným vynucovaním politiky v značkách.

Vysoko závažná zraniteľnosť CVE-2026-0901 v komponente **Blink** súvisí s nevhodnou implementáciou nešpecifikovaných prvkov.

Komponent **Background Fetch API** obsahuje vysoko závažnú zraniteľnosť CVE-2026-1504, ktorá súvisí s nevhodnou implementáciou nešpecifikovaných prvkov.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows verzie staršej ako 144.0.7559.109/.110
- Google Chrome pre Mac verzie staršej ako 144.0.7559.109/.110
- Google Chrome pre Linux verzie staršej ako 144.0.7559.109

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 144.0.7559.109/.110 a Linux aspoň na verziu 144.0.7559.109.

ZDROJE:

- https://chromereleases.googleblog.com/2026/01
- https://chromereleases.googleblog.com/2026/01/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2026/01/stable-channel-update-for-desktop_13.html
- https://chromereleases.googleblog.com/2026/01/stable-channel-update-for-desktop_20.html
- https://chromereleases.googleblog.com/2026/01/stable-channel-update-for-desktop_27.html

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 neopravila žiadnu kritickú ani vysoko závažnú zraniteľnosť vo frameworku .NET.

ZDROJE:

- https://msrc.microsoft.com/update-guide/en-us

ORACLE JAVA

Spoločnosť Oracle v mesiaci október vydala bezpečnostné aktualizácie, ktoré opravujú 4 vysoko závažné zraniteľnosti v rámci Oracle Java SE.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2025-43368 sa nachádza v komponente JavaFX WebKitGTK. Neautentifikovaný vzdialený útočník by mohol zneužiť dealokované miesto v pamäti pre **vyvolanie pádu aplikácie**.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2025-7425 sa nachádza v komponente JavaFX libxslt. Chyba súvisí s nesprávny manažmentom pamäte pri mazaní niektorých atribútov. Neautentifikovaný lokálny útočník by mohol zneužiť dealokované miesto v pamäti pre **vyvolanie pádu aplikácie**.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2026-21945 sa nachádza v komponente Security. Neautentifikovaný vzdialený útočník by jej zneužitím mohol spôsobiť opakovaný **pád aplikácie**.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2026-21932 sa nachádza v komponentoch JavaFX a AWT. Neautentifikovaný vzdialený útočník by ju mohol zneužiť pre získanie **prístupu k citlivým dátam** a možnosti **ich modifikácie a mazania**. Na to potrebuje interakciu obete.

ZRANITEĽNÉ SYSTÉMY:

- Oracle Java SE: 8u471, 8u471-b50, 8u471-perf, 11.0.29, 17.0.17, 21.0.9, 25.0.1
- Oracle GraalVM for JDK: 17.0.17, 21.0.9
- GraalVM Enterprise Edition: 21.3.16

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/cpujan2026.html#AppendixJAVA
- https://nvd.nist.gov/vuln/detail/CVE-2025-43368
- https://nvd.nist.gov/vuln/detail/CVE-2025-7425
- https://nvd.nist.gov/vuln/detail/CVE-2026-21945
- https://nvd.nist.gov/vuln/detail/CVE-2026-21932

INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

MONGOBLEED: AKTÍVNE ZNEUŽÍVANÁ ZRANITEĽNOSŤ MONGODB SERVER UMOŽŇUJE ČÍTAŤ PAMÄŤ

Vývojári MongoDB Server opravili vysoko závažnú zraniteľnosť umožňujúcu vzdialenému neautentifikovanému útočníkovi manipulovať premenné v hlavičkách požiadaviek a získavať tak citlivé informácie z pamäte na halde (angl. heap) v rámci operačnej pamäte. Zraniteľnosť je aktívne zneužívaná. Viac informácií na stránke.

PLATFORMA COOLIFY OBSAHUJE 11 KRITICKÝCH ZRANITEĽNOSTÍ

Vývojári open-source platformy pre manažovanie serverov, aplikácií a databáz Coolify opravili 11 kritických chýb, ktoré môžu viesť k obídeniu autentifikácie, vzdialenému vykonaniu kódu a

úplnému kompromitovaniu hostiteľského systému. Chyby zabezpečenia súvisia najmä s neošetrenými parametrami, nad ktorými má kontrolu používateľ. Tieto aplikácia preberá priamo do príkazov pre shell. Viac informácií na stránke.

TREND MICRO APEX CENTRAL OBSAHUJE TRI ZÁVAŽNÉ ZRANITEĽNOSTI

Spoločnosť Trend Micro vydala bezpečnostné aktualizácie svojho produktu Apex Central pre Windows, ktoré opravujú 3 zraniteľnosti, z čoho 1 je označená ako kritická. Kritická zraniteľnosť umožňuje neautentifikovanému útočníkovi vykonávať vzdialene kód s oprávneniami úrovne SYSTEM. Ďalšie dve zraniteľnosti by mohol vzdialený neautentifikovaný útočník zneužiť na zneprístupnenie služby. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V NPM KNIŽNICIACH JSPDF A ADONISJS

Bezpečnostní výskumníci našli kritické zraniteľnosti vo dvoch knižniciach NPM – jsPDF na generovanie PDF dokumentov a MVC knižnici AdonisJS. Ide o často využívané knižnice, ktoré majú spolu viac ako 3,5 milióna stiahnutí týždenne. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ FORTINET FORTISIEM

Spoločnosť Fortinet opravila kritickú zraniteľnosť FortiSIEM, ktorá umožňuje kontrolovať obsah požiadaviek TCP a následne vykonávať kód a príkazy s oprávneniami administrátora, bez potreby autentifikácie. Viac informácií na stránke.

ZRANITEĽNOSŤ NPM KNIŽNICE BINARY-PARSER UMOŽŇUJE VZDIALENÉ VYKONANIE KÓDU

Vývojári NPM knižnice pre parsovanie binárnych dát binary-parser vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú kritickú zraniteľnosť CVE-2026-1245. Táto spočíva v nedostatočnom overovaní používateľských vstupov, čo by mohol vzdialený neautentifikovaný útočník zneužiť na vzdialené vykonanie kódu JavaScript s privilégiami procesu Node.js. Viac informácií na stránke.

ZRANITEĽNOSŤ WP MODULU ADVANCED CUSTOM FIELDS: EXTENDED UMOŽŇUJE ZÍSKANIE ADMINISTRÁTORSKEJ KONTROLY

Vývojári modulu Advanced Custom Fields: Extended pre WordPress vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú kritickú zraniteľnosť. CVE-2025-14533 spočíva v nesprávnej reštrikcii rolí v rámci formulára pre tvorbu a editáciu používateľov. Vzdialený neautentifikovaný útočník by ju mohol zneužiť na získanie administrátorského prístupu a úplnej kontroly nad systémom. Viac informácií na stránke.

CISCO OPRAVILA KRITICKÚ ZERO-DAY ZRANITEĽNOSŤ VO VIACERÝCH PRODUKTOCH

Spoločnosť Cisco opravila kritickú aktívne zneužívanú zraniteľnosť CVE-2026-20045 vo viacerých svojich produktoch. Zraniteľnosť umožňuje neautentifikovanému útočníkovi vzdialene vykonávať systémové príkazy a získať oprávnenia používateľa root. Viac informácií na stránke.

TELNETD OBSAHUJE KRITICKÚ ZRANITEĽNOSŤ

Nástroj telnetd v balíku GNU InetUtils nesanitizuje používateľské vstupy v niektorých premenných. Tým umožňuje injektovať hodnoty vedúce k obídeniu autentifikácie a získanie prístupu s oprávneniami používateľa root. V nástroji sa nachádza vyše 10 rokov. Viac informácií na stránke.