MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

FEBRUÁR 2026

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci február 1 kritickú a 30 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritická zraniteľnosť CVE-2026-26119 v súčasti Windows Admin Center súvisí s nevhodným spôsobom autentifikácie. Vzdialený útočník s nízkymi oprávneniami ju môže zneužiť na **navýšenie svojich oprávnení** na úroveň aktuálneho používateľa aplikácie.

Vysoko závažné zraniteľnosti CVE-2026-21244, CVE-2026-21247 a CVE-2026-21248 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 11 Version 26H1 for ARM64-based Systems
- Windows 11 version 26H1 for x64-based Systems
- Windows Admin Center
- Windows App for Mac
- 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-2026-26119

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 február bezpečnostné aktualizácie, ktoré opravujú 1 kritickú a 7 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritickú zraniteľnosť **Microsoft Teams** s označením CVE-2026-21535 môže neautorizovaný vzdialený útočník zneužiť na **získanie citlivých informácií**. Chyba zabezpečenia súvisí s nevhodnou kontrolou prístupov. Spoločnosť Microsoft zraniteľnosť opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre jej odstránenie.

Vysoko závažné zraniteľnosti spočívajú v pretečení vyrovnávacej pamäte na halde, deserializácii nedôveryhodných dát, možnosti čítania pamäte mimo povolené hodnoty, neošetrení používateľských vstupov a exponovaní citlivých informácií. Predmetné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu, eskaláciu oprávnení, 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 Excel 2016 (32-bit edition)
- Microsoft Excel 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 2016 (32-bit edition)
- Microsoft Outlook 2016 (64-bit edition)
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription Edition
- Microsoft Teams
- Microsoft Word 2016 (32-bit edition)
- Microsoft Word 2016 (64-bit edition)
- Office Online Server
- Windows Notepad

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-2026-21535

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 február 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 február opravila 34 vysoko závažných zraniteľností v línii internetových prehliadačov Firefox a Firefox ESR.

Zraniteľnosti CVE-2026-2032 a CVE-2026-2634 sa nachádzajú v línii Firefox pre iOS a umožňujú útočníkovi falšovať dôveryhodné stránky. Prvá súvisí s možnosťou vyvolať pomocou škodlivého

skriptu prerušenie načítania webovej stránky na novej záložke, druhá s možnosťou desynchronizovať adresový riadok s webovým obsahom.

Zraniteľnosť CVE-2026-2447 v komponente libvpx línií Firefox a Firefox ESR súvisí s pretečením medzipamäte na halde.

Päť zraniteľností v líniách Firefox a Firefox ESR súvisí s nesprávne nastavenými limitnými podmienkami. CVE-2026-2757 sa nachádza v komponente WebRTC: Audio/Video, CVE-2026-2759 v Graphics: ImageLib, CVE-2026-2760 v Graphics: WebRender, CVE-2026-2773 vo Web Audio, CVE-2026-2776 v Telemetry a CVE-2026-2778 v komponente DOM: Core & HTML. Tri z nich umožňujú útočníkovi **uniknúť zo sandboxu**.

Línia Firefox obsahuje 13 zraniteľností, ktoré umožňujú **použitie dealokovaného miesta v pamäti**. Zraniteľnosť CVE-2026-2758 sa nachádza v komponente JavaScript: GC, CVE-2026-2763, CVE-2026-2764 v JavaScript Engine, CVE-2026-2766 v JavaScript Engine: JIT a CVE-2026-2767 v JavaScript: WebAssembly. Zraniteľnosť CVE-2026-2769 je obsiahnutá v komponente Storage: IndexedDB, CVE-2026-2770 v DOM: Bindings (WebIDL) a CVE-2026-2772 v Audio/Video: Playback. Zraniteľnosti CVE-2026-2795 a CVE-2026-2797 sa nachádzajú v JavaScript: GC, CVE-2026-2798 a CVE-2026-2799 v DOM: Core & HTML. Prvých deväť z nich obsahuje aj línia Firefox ESR.

Únik informácií môže spôsobiť vysoko závažná zraniteľnosť CVE-2026-2794 v línii Firefox. Súvisí s chybou neinicializovanej pamäte.

Únik zo sandboxu umožňujú vysoko závažné zraniteľnosti línií Firefox a Firefox ESR CVE-2026-2761 v komponente Graphics: WebRender a CVE-2026-2768 v Storage: IndexedDB.

Línie Firefox a Firefox ESR obsahujú tiež zraniteľnosť CVE-2026-2762 v komponente JavaScript: Standard Library a CVE-2026-2774 v Audio/Video. Tieto súvisia s pretečením celočíselnej premennej.

Zraniteľnosť CVE-2026-2796 v línii Firefox sa nachádza v komponente JavaScript: WebAssembly. Vyplýva z chybnej kompilácie v nástroji JIT.

Línie Firefox a Firefox ESR obsahujú tiež zraniteľnosť CVE-2026-2771, ktorá tkvie v nedefinovanom správaní komponentu DOM: Core & HTML.

Ďalšia zraniteľnosť CVE-2026-2775 v líniách Firefox a Firefox ESR umožňuje **obídenie nešpecifikovanej mitigácie** v komponente DOM: HTML Parser.

Zraniteľnosť CVE-2026-2777 komponentu Messaging System **umožňuje eskalovať oprávnenia**. Prítomná je v líniách Firefox aj Firefox ESR.

Identifikátor CVE-2026-2807 v línii Firefox indikátory CVE-2026-2792 a CVE-2026-2793 v líniách Firefox a Firefox ESR opisujú sady chýb pri narábaní s pamäťou. Tieto zraniteľnosti ovplyvňujú bezpečnosť pamäte a môžu viesť ku **poškodeniu pamäte** alebo možnosti **vykonávať kód**.

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox verzie staršie ako 148
- Mozilla Firefox ESR verzie staršej ako 115.33 a 140.8
- Mozilla Firefox pre iOS verzie staršej ako 147.4

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 148, Firefox ESR na verziu 115.33 alebo 140.8 a Firefox pre iOS na verziu 147.4.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-09/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-10/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-12/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/

GOOGLE CHROME

V mesiaci február spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 11 vysoko závažných zraniteľností.

Komponent **V8** obsahuje dve vysoko závažné zraniteľnosti. CVE-2026-1862 súvisí so zámenou typu premennej, CVE-2026-0900 s pretečením celočíselnej premennej.

Vysoko závažná zraniteľnosť CVE-2026-1861 v komponente **libvpx** súvisí s pretečením vyrovnávacej pamäte na halde.

Komponent **CSS** obsahuje dve vysoko závažné zraniteľnosti CVE-2026-2313 a CVE-2026-2441, ktoré umožňujú opätovné použitie dealokovanej pamäte.

Vysoko závažná zraniteľnosť CVE-2026-2314 v komponente **Codecs** súvisí s pretečením vyrovnávacej pamäte na halde.

Komponent **WebGPU** obsahuje vysoko závažnú zraniteľnosť CVE-2026-2315, ktorá vyplýva z nevhodnej implementácie nešpecifikovaných prvkov.

Vysoko závažná zraniteľnosť CVE-2026-2648 v komponente **PDFium** súvisí s pretečením vyrovnávacej pamäte na halde.

Vysoko závažná zraniteľnosť CVE-2026-3061 v komponente **Media** umožňuje čítať obsah pamäte mimo povolené hodnoty.

Čítanie obsahu pamäte mimo povolené hodnoty dovoľuje rovnako vysoko závažná zraniteľnosť CVE-2026-3062 v komponente **Tint**.

Komponent **DevTools** obsahuje vysoko závažnú zraniteľnosť CVE-2026-3063, ktorá vyplýva z nevhodnej implementácie nešpecifikovaných prvkov.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows verzie staršej ako 145.0.7632.116/117
- Google Chrome pre Mac verzie staršej ako 145.0.7632.116/117
- Google Chrome pre Linux verzie staršej ako 145.0.7632.116

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 145.0.7632.116/117 a Linux aspoň na verziu 145.0.7632.116.

ZDROJE:

- https://chromereleases.googleblog.com/2026/02
- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_10.html

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_13.html
- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_18.html
- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_23.html

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 jednu vysoko závažnú zraniteľnosť vo frameworku .NET.

CVE-2026-21218 spočíva v nesprávnom narábaní s chýbajúcim nešpecifikovaným špeciálnym prvkom. Neautorizovanému vzdialenému útočníkovi umožňuje obchádzať validáciu kritických hlavičiek a vykonávať útoky typu spoofing.

ZRANITEĽNÉ SYSTÉMY:

- .NET 10.0 installed on Linux
- .NET 10.0 installed on Mac OS
- .NET 10.0 installed on Windows
- .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

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-2026-21218

ORACLE JAVA

Spoločnosť Oracle plánuje vydať veľkú sadu opráv 21. apríla 2026.

ZDROJE:

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

INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

ZRANITEĽNOSŤ VM2 PRE NODE.JS UMOŽŇUJE OBÍSŤ SANDBOXING

Vývojári knižnice vm2 pre Node.js s funkcionalitou sandboxingu opravili kritickú chybu, ktorá útočníkom umožňuje uniknúť zo sandboxu a vykonávať ľubovoľný kód. Viac informácií na stránke.

FORTINET OPRAVIL AKTÍVNE ZNEUŽÍVANÚ KRITICKÚ ZRANITEĽNOSŤ VO FORTICLOUD SSO

Spoločnosť Fortinet vydala bezpečnostné aktualizácie FortiOS, FortiManager, FortiProxy a FortiAnalyzer, ktoré opravujú aktívne zneužívanú kritickú zraniteľnosť vo FortiCloud SSO. CVE-2026-24858 by vzdialený neautentifikovaný útočník mohol zneužiť na obídenie autentifikácie na zraniteľné zariadenia. Viac informácií na stránke.

KRITICKÉ ZERO-DAY ZRANITEĽNOSTI V PRODUKTE IVANTI ENDPOINT MANAGER MOBILE

Spoločnosť Ivanti vydala bezpečnostné aktualizácie pre Ivanti Endpoint Manager Mobile, ktoré opravujú dve aktívne zneužívané kritické zero-day zraniteľnosti. CVE-2026-1281 a CVE-2026-1340 umožňujú injekciu kódu. Vzdialený neautentifikovaný útočník by ich mohol zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ FORTICLIENTEMS 7.4.4

Fortinet FortiClientEMS verzie 7.4.4 obsahuje zraniteľnosť, ktorá umožňuje vykonávať SQL injekciu prostredníctvom nesanitizovaných HTTP požiadaviek. Vzdialený neautorizovaný útočník môže získať schopnosť vykonávať kód a príkazy. Viac informácií na stránke.

ZRANITEĽNOSŤ WINDOWS NOTEPAD UMOŽŇUJE VZDIALENÉ VYKONANIE KÓDU PROSTREDNÍCTVOM DOKUMENTOV MARKDOWN

Spoločnosť Microsoft v rámci Patch Tuesday vo februári 2026 opravila vysoko závažnú bezpečnostnú zraniteľnosť v textovom editore Windows Notepad. CVE-2026-20841 umožňuje vzdialené vykonanie kódu prostredníctvom dokumentu Markdown. Viac informácií na stránke.

APPLE OPRAVILA AKTÍVNE ZNEUŽÍVANÚ ZERO-DAY ZRANITEĽNOSŤ SVOJICH OPERAČNÝCH SYSTÉMOV

Spoločnosť Apple vydala bezpečnostné aktualizácie svojich operačných systémov iOS, iPadOS, macOS, tvOS, watchOS a visionOS, ktoré opravujú viacero zraniteľností, z čoho jedna je označená ako aktívne zneužívaná zero-day. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ MODULU WPVIVID BACKUP & MIGRATION PRE WORDPRESS UMOŽŇUJE VYKONÁVAŤ KÓD

Vývojári modulu WPvivid Backup & Migration pre WordPress opravili kritickú zraniteľnosť, ktorá umožňuje útočníkom zneužiť proces výmeny šifrovacích kľúčov na podvrhnutie ľubovoľného škodlivého súboru a jeho nahratie do ľubovoľného verejne dostupného adresáru. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ BEYONDTRUST REMOTE SUPPORT A PRIVILEGED REMOTE ACCESS UMOŽŇUJE VYKONÁVAŤ PRÍKAZY

Vývojári BeyondTrust Remote Support a Privileged Remote Access opravili kritickú zraniteľnosť, ktorá umožňuje vzdialenému neautentifikovanému útočníkovi vykonávať systémové príkazy na zraniteľnom systéme. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V ROZŠÍRENIACH VISUAL STUDIO CODE UMOŽŇUJÚ VYKONÁVAŤ KÓD A EXFILTROVAŤ DÁTA

Výskumníci zo spoločnosti Ox Security identifikovali viaceré závažné zraniteľnosti v populárnych rozšíreniach pre Visual Studio Code (VSCode). Útočníci ich môžu zneužiť na kradnutie lokálnych súborov a vzdialené vykonávanie kódu priamo v prostredí vývojára. Viac informácií na stránke.