MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

DECEMBER 2025

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci december 39 vysoko závažných zraniteľností v operačných systémoch Windows.

Vysoko závažné zraniteľnosti CVE-2025-54100, CVE-2025-62456, CVE-2025-62549 a CVE-2025-64678 by vzdialený útočník mohol zneužiť na **vzdialené vykonanie kódu** a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Spoločnosť opravila aj vysoko závažnú zraniteľnosť CVE-2025-9491 v narábaní so súbormi LNK v systémoch Windows, ktorá je **aktívne zneužívaná** aspoň od roku 2017. Táto chyba zabezpečenia môže viesť ku **vzdialenému vykonaniu kódu**.

Ostatné zraniteľnosti vysokej závažnosti možno zneužiť na eskaláciu privilégií, zneprístupnenie služby (DoS) a získanie prístupu k citlivým informáciám.

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 11 Version 25H2 for ARM64-based Systems
- Windows 11 Version 25H2 for x64-based Systems
- Windows Admin Center
- 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://csirt.sk/posts/2984.html

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 skončí 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 december bezpečnostné aktualizácie, ktoré opravujú 4 kritické a 12 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritické zraniteľnosti CVE-2025-62554 a CVE-2025-62557 v produkte **Microsoft Office** môže neautorizovaný vzdialený útočník zneužiť na lokálne **vykonanie ľubovoľného škodlivého kódu**. Zraniteľnosti spočívajú v zámene typu premennej a možnosti použitia dealokovaného miesta v pamäti. Zneužiť ich možno zaslaním škodlivého odkazu obeti, ktorá môže, no v niektorých prípadoch nemusí na odkaz kliknúť. Útočným vektorom môže byť aj náhľad dokumentu (Preview Pane).

Kritickú zraniteľnosť **Microsoft Purview eDiscovery** s označením CVE-2025-64676 môže autorizovaný útočník zneužiť na vzdialené **vykonanie škodlivého kódu**. Chyba zabezpečenia súvisí s nedostatočnou kontrolou pri generovaní kódu, čo umožňuje injektovať kód. Spoločnosť Microsoft zraniteľnosť opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre jej odstránenie.

Kritická zraniteľnosť **Microsoft Office Out-of-Box Experience** s označením CVE-2025-64677 súvisí s nedostatočnou kontrolou používateľských vstupov pri generovaní webstránky. Vzdialený neautorizovaný útočník ju môže zneužiť na **maskovanie obsahu** pri útokoch typu **XSS**. Spoločnosť Microsoft zraniteľnosť opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre jej odstránenie.

Vysoko závažné zraniteľnosti spočívajú v dereferencii nedôveryhodného ukazovateľa, možnosti čítania pamäte mimo povolené hodnoty, použití dealokovaného miesta v pamäti, možnosti vykonávania útokov XSS (neošetrení používateľských vstupov) a možnosti prechádzania medzi priečinkami. Predmetné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu** 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 Access 2016 (32-bit edition)
- Microsoft Access 2016 (64-bit edition)
- 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 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 Purview
- 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
- Office Out-of-Box Experience

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-2025-62554
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62557
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-64676
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-64677

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 december 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 december opravila 7 vysoko závažných zraniteľností v línii internetových prehliadačov Firefox a Firefox ESR.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť umožňujúcu použitie dealokovaného miesta v pamäti CVE-2025-14321, ktorá sa nachádza v komponente WebRTC: Signaling.

Zraniteľnosť CVE-2025-14322 v línii Firefox a Firefox ESR v komponente Graphics: CanvasWebGL vzniká kvôli nesprávne nastaveným limitným podmienkam. Útočníkovi umožňuje **uniknúť zo sandboxu**.

Zraniteľnosť CVE-2025-14323 v komponente DOM: Notifications línií Firefox a Firefox ESR dovoľuje **eskalovať oprávnenia**.

Zraniteľnosti CVE-2025-14324 a CVE-2025-14325 v líniách Firefox a Firefox ESR vznikajú chybnou kompiláciou v nástroji JIT.

Línia Firefox obsahuje tiež zraniteľnosť CVE-2025-14860, ktorá vyplýva z možnosti použitia dealokovanej pamäte. Nachádza sa v komponente Disability Access API.

Identifikátor CVE-2025-14861 v línii Firefox 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 146.0.1
- Mozilla Firefox ESR verzie staršej ako 115.31 a 140.6

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 146.0.1 a Firefox ESR na verziu 115.31 alebo 140.6.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-92/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-93/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-94/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-98/

GOOGLE CHROME

V mesiaci december spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 7 vysoko závažných zraniteľností.

Komponent V8 obsahuje dve vysoko závažné zraniteľnosti. CVE-2025-14766 súvisí s možnosťou zápisu do pamäte mimo povolené hodnoty a CVE-2025-13630 súvisí so zámenou typu premennej.

Vysoko závažná zraniteľnosť CVE-2025-14765 v komponente WebGPU súvisí s možnosťou použitia dealokovaného miesta v pamäti.

Vysoko závažná zraniteľnosť CVE-2025-14174 v komponente ANGLE súvisí s možnosťou prístupu k pamäti mimo povolené hodnoty.

Zraniteľnosti CVE-2025-13631 a CVE-2025-13632 vyplývajú z nevhodnej implementácie nešpecifikovaných prvkov. Nachádzajú sa v komponentoch Google Updater a DevTools.

Komponent Digital Credentials obsahuje vysoko závažnú zraniteľnosť CVE-2025-13633, ktorá súvisí s možnosťou použitia dealokovaného miesta v pamäti.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows verzie staršej ako 143.0.7499.146/.147
- Google Chrome pre Mac verzie staršej ako 143.0.7499.146/.147
- Google Chrome pre Linux verzie staršej ako 143.0.7499.146

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 143.0.7499.146/.147 a Linux aspoň na verziu 143.0.7499.146.

ZDROJE:

- https://chromereleases.googleblog.com/2025/12
- https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop_10.html
- https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop_16.html
- https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop_18.html

4. ADOBE ACROBAT A READER

V mesiaci december spoločnosť Adobe opravila 2 vysoko závažné zraniteľnosti v produktoch Adobe Acrobat a Reader.

Zraniteľnosť CVE-2025-64785 súvisí s možnosťou externého zadávania ciest ku zdrojom systému nedôveryhodnej a možno ju zneužiť na vykonanie ľubovoľného kódu.

Zraniteľnosť CVE-2025-64899 spočíva v neošetrenom narábaní s pamäťou, čo umožňuje jej čítanie mimo povolené hodnoty. Možno ju zneužiť na vykonanie ľubovoľného kódu.

ZRANITEĽNÉ SYSTÉMY:

- Acrobat DC a Acrobat Reader DC verzie 25.001.20982 pre Windows a Mac, a staršie
- Acrobat 2020 a Acrobat Reader 2020 pre Windows verzie 20.005.30793 a Mac verzie 20.005.30803 a staršie
- Acrobat 2024 pre Windows verzie 24.001.30264 a Mac verzie 24.001.30273 a staršie

ODPORÚČANIA:

Odporúčame aktualizáciu aspoň na verziu:

- Acrobat DC a Acrobat Reader DC pre Windows a Mac 25.001.20997
- Acrobat 2020 a Acrobat Reader 2020 pre Windows a Mac 20.005.30838
- Acrobat 2024 pre Windows 24.001.30307 a Mac 24.001.30308

ZDROJE:

- https://helpx.adobe.com/security/security-bulletin.html#acrobat
- https://helpx.adobe.com/security/products/acrobat/apsb25-119.html

5. FRAMEWORKY

MICROSOFT .NET FRAMEWORK

V mesiaci december 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 plánuje vydať veľkú sadu opráv 20. januára 2026.

ZDROJE:

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

INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

KRITICKÁ ZRANITEĽNOSŤ REACT SERVER COMPONENTS UMOŽŇUJE VYKONÁVAŤ KÓD

Vývojári platformy JavaScript React opravili kritickú zraniteľnosť v React Server Components, ktorá umožňuje vzdialené vykonávanie kódu na serveri. Zasiahnuté sú viaceré balíčky npm, vrátane platformy Next.js. Zraniteľnosť dostala pomenovanie React2Shell. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ APACHE TIKA UMOŽŇUJE INJEKTOVAŤ XML

Vývojári Apache Tika vydali opravné aktualizácie pre viacero modulov, do ktorých je možné injektovať externé entity XML. Zneužitím opravenej zraniteľnosti môže útočník získať schopnosť čítať citlivé dáta alebo vzdialene vykonávať kód. Viac informácií na stránke.

APPLE OPRAVILA AKTÍVNE ZNEUŽÍVANÉ ZRANITEĽNOSTI SVOJICH OS A PREHLIADAČA

Apple vydala aktualizácie na opravu dvoch zero-day zraniteľností, ktoré sa nachádzajú v nástroji WebKit prehliadača Safari a ďalších prehliadačov na iOS a knižnici ANGLE pre Google Chrome pre Mac. CVE-2025-43529 umožňuje vykonávanie ľubovoľného kódu a možno ju zneužiť spracovaním škodlivého webového obsahu. CVE-2025-14174 môže viesť k poškodeniu pamäte. Viac informácií na stránke.

ZRANITEĽNOSTI FREEPBX UMOŽŇUJÚ ZÍSKAŤ KONTROLU NAD SYSTÉMOM

Vývojári FreePBX opravili jednu kritickú a dve vysoko závažné zraniteľnosti v aplikácii FreePBX Endpoint Manager. Kritická zraniteľnosť umožňuje obísť autentifikáciu, zatiaľ čo ostatné dve dovoľujú získavať a meniť dáta v SQL databáze a nahrávať ľubovoľné súbory. Viac informácií na stránke.

KRITICKÚ ZRANITEĽNOSŤ CISCO ASYNCOS AKTÍVNE ZNEUŽÍVAJÚ VO VIACERÝCH KAMPANIACH

Spoločnosť Cisco varovala pred aktívnym zneužívaním kritickej zero-day zraniteľnosti v produktoch Cisco SEG (Secure Email Gateway) a SEWM (Secure Email and Web Manager). Zraniteľnosť s identifikátorom CVE-2025-20393 v operačnom systéme AsyncOS umožňuje

vzdialene vykonávať systémové príkazy a kompromitovať zraniteľný systém. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ ZRANITEĽNOSŤ SONICWALL SMA1000

Spoločnosť SonicWall vydala bezpečnostné aktualizácie pre zariadenia SonicWall SMA1000, ktoré opravujú aktívne zneužívanú zraniteľnosť. Zraniteľnosť strednej závažnosti CVE-2025-40602 spočíva v nedostatočnej autorizácii v rámci konzoly AMC (Application Management Console) a lokálny útočník by ju mohol zneužiť na eskaláciu privilégií. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ HEWLETT PACKARD ENTERPRISE ONEVIEW

Spoločnosť HPE varuje pred kritickou zraniteľnosťou manažmentovej platformy OneView, ktorá umožňuje vzdialené vykonávanie kódu. Viac informácií na stránke.