MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

NOVEMBER 2025

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci november 3 kritické a 36 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritickú zraniteľnosť CVE-2025-60716 v komponente **Windows DirectX** môže lokálny útočník s nízkymi oprávneniami zneužiť na **navýšenie svojich oprávnení** na úroveň **SYSTEM**. Na to potrebuje vyhrať súbeh procesov. Spolupráca obete nie je potrebná.

Súčasť **Windows Graphics Component** obsahuje kritickú zraniteľnosť s identifikátorom CVE-CVE-2025-60724. Zraniteľnosť spočíva v pretečení vyrovnávacej pamäte haldy. Neautorizovaný vzdialený útočník ju môže zneužiť na **vykonanie ľubovoľného kódu**. Na to potrebuje vytvoriť súbor so špeciálne upravenými metadátami, ktorý otvorí obeť, alebo ktorý nahrá do webovej služby.

Kritická zraniteľnosť s identifikátorom CVE-2025-62459 v komponente súčasti **Microsoft Defender Portal** spočíva v nesprávnej sanitizácii používateľských vstupov. Vzdialený neautorizovaný útočník ju môže zneužiť na , čo umožňuje vykonávanie **útokov typu XSS**. Spoločnosť zraniteľnosť opravila a nevyžaduje sa akcia zo strany zákazníkov.

Vysoko závažné zraniteľnosti CVE-2025-62452, CVE-2025-60715 a CVE-2025-60714 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) a získanie prístupu k citlivým informáciám.

Zraniteľné systémy:

- Microsoft 365 Defender Portal
- 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 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-2025-60716
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-60724
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62459

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. Po rokovaní s organizáciou Euroconsumers však v Európskom hospodárskom priestore predĺži 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:

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 november bezpečnostné aktualizácie, ktoré opravujú 2 kritické a 13 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritickú zraniteľnosť CVE-2025-59245 v produkte **Microsoft Sharepoint Online** môže neautorizovaný vzdialený útočník zneužiť na **eskalovanie oprávnení**. Zraniteľnosti spočívajú v deserializácii nedôveryhodných dát. Spoločnosť Microsoft zraniteľnosť opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre jej odstránenie.

Kritická zraniteľnosť **Microsoft Office** s označením CVE-2025-62199 súvisí s možnosťou použitia dealokovaného miesta v pamäti. Neautorizovaný útočník ju môže zneužiť na lokálne **vykonanie ľubovoľného škodlivého kódu**. Potrebuje na to interakciu obete, ktorá otvorí špeciálne vytvorený škodlivý súbor. Útočným vektorom môže byť aj náhľad dokumentu (Preview Pane).

Vysoko závažné zraniteľnosti spočívajú v zámene typu premennej, dereferencii nedôveryhodného ukazovateľa, možnosti čítania medzipamäte mimo povolené hodnoty, použití dealokovaného miesta v pamäti, deserializácii nedôveryhodných dát, pretečení medzipamäte haldy, exponovaní citlivých údajov a možnosti prechádzania medzi priečinkami. Predmetné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu, získanie citlivých informácií, eskaláciu privilégií** a **eskalovanie oprávnení**.

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 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 SharePoint Enterprise Server 2016
- Microsoft SharePoint Online
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription Edition
- Office Online Server
- OneDrive for Android

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-2025-59245
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62199

Koniec podpory pre Office 2016 a Office 2019

Spoločnosť Microsoft tento rok plánovane zruší podporu pre Office 2016 a Office 2019. Po dátume 14. novembra 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 november 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 november opravila 9 vysoko závažných zraniteľností v línii internetových prehliadačov Firefox a Firefox ESR.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť súbehu procesov CVE-2025-13012, ktorá sa nachádza v komponente Graphics.

Zraniteľnosť CVE-2025-13016 v línii Firefox a Firefox ESR 140.4 v komponente JavaScript WebAssembly vzniká kvôli nesprávne nastaveným limitným podmienkam.

Zraniteľnosti CVE-2025-13021, CVE-2025-13022 a CVE-2025-13025 v komponente Graphics WebGPU línie Firefox súvisia s nesprávne nastavenými limitnými podmienkami.

V línii Firefox sa nachádzajú aj zraniteľnosti CVE-2025-13023 a CVE-2025-13026. Súvisia s nesprávne nastavenými limitnými podmienkami v komponente Graphics WebGPU. Útočníkovi umožňujú uniknúť zo sandboxu.

Zraniteľnosť CVE-2025-13024 v línii Firefox vzniká chybnou kompiláciou v nástroji JIT.

Identifikátor CVE-2025-13027 v línii Firefox. Táto zraniteľnosť ovplyvňuje bezpečnosť pamäte a môže viesť ku poškodeniu pamäte alebo možnosti vykonávať kód.

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox a Firefox pre iOS verzie staršie ako 145
- Mozilla Firefox ESR verzie staršej ako 115.30 a 140.5

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 145 a Firefox ESR na verziu 115.30 alebo 140.5.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-87/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-88/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-89/

GOOGLE CHROME

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

Komponent V8 obsahuje viacero vysoko závažných zraniteľností. CVE-2025-13223 a CVE-2025-13224 súvisia so zámenou typu premennej. Prvá je aktívne zneužívaná. CVE-2025-12727 a CVE-2025-13042 sú zapríčinené nevhodnou implementáciou nešpecifikovaných funkcionalít.

Vysoko závažná zraniteľnosť CVE-2025-12725 v komponente WebGPU súvisí s možnosťou zápisu do pamäte mimo povolené hodnoty.

Vysoko závažná zraniteľnosť CVE-2025-12726 v komponente Views vyplýva z nevhodnej implementácie nešpecifikovaných prvkov.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows verzie staršej ako 142.0.7444.175/.176
- Google Chrome pre Mac verzie staršej ako 142.0.7444.176
- Google Chrome pre Linux verzie staršej ako 142.0.7444.175

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows aspoň na verziu 142.0.7444.175/.176, Mac aspoň na verziu 142.0.7444.176 a Linux aspoň na verziu 142.0.7444.175.

ZDROJE:

- https://chromereleases.googleblog.com/2025/11
- https://chromereleases.googleblog.com/2025/11/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2025/11/stable-channel-update-for-desktop_11.html
- https://chromereleases.googleblog.com/2025/11/stable-channel-update-for-desktop_17.html

4. ADOBE ACROBAT A READER

V mesiaci november 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 november 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

ZRANITEĽNOSTI CHATGPT UMOŽŇOVALI ÚNIK CITLIVÝCH ÚDAJOV CEZ "INDIRECT PROMPT INJECTION"

Bezpečnostní výskumníci zo spoločnosti Tenable zverejnili informácie o siedmich zraniteľnostiach v systéme OpenAI ChatGPT, ktoré mohli útočníkom umožniť realizáciu tzv. indirect prompt injection útokov. Tieto útoky umožňujú získať prístup k citlivým informáciám používateľov prostredníctvom manipulácie vstupov, ktoré model následne spracováva. Viac informácií na stránke.

ZRANITEĽNOSŤ V KONTAJNERI RUNC UMOŽŇUJE ÚNIK Z IZOLOVANÉHO PROSTREDIA

Bezpečnostný výskumník zo spoločnosti SUSE objavil tri zraniteľnosti, ktoré umožňujú lokálnemu útočníkovi za určitých podmienok uniknúť z izolovaného prostredia softvérového kontajneru a získať administrátorské (root) oprávnenia v hostiteľskom systéme. Viac informácií na stránke.

ZRANITEĽNOSŤ MODULU WORDPRESS W3 TOTAL CACHE UMOŽŇUJE VZDIALENÉ VYKONANIE PRÍKAZOV PHP

Vývojári modulu WordPress W3 Total Cache vydali bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť. CVE-2025-9501 možno zneužiť na vzdialené vykonanie PHP príkazov a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

FORTINET OPRAVIL 2 AKTÍVNE ZNEUŽÍVANÉ ZRANITEĽNOSTI VO WAF FORTIWEB

Spoločnosť Fortinet vydala bezpečnostné aktualizácie svojho webového aplikačného firewallu FortiWeb, ktoré opravujú 2 aktívne zneužívané zero day zraniteľnosť. Zraniteľnosti s identifikátormi CVE-2025-64446 a CVE-2025-58034 možno zneužiť na získanie úplnej kontroly nad systémom. Viac informácií na stránke.

ASUS OPRAVIL KRITICKÚ ZRANITEĽNOSŤ V ROUTEROCH SÉRIE DSL

Spoločnosť ASUS vydala bezpečnostné aktualizácie firmvéru routerov série DSL, ktoré opravujú kritickú zraniteľnosť. CVE-2025-59367 možno zneužiť na získanie neoprávneného prístupu do systému a úplné narušenie dôvernosti, integrity a dostupnosti zariadenia. Viac informácií na stránke.