MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

SEPTEMBER 2025

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci september 7 kritických a 54 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritickú zraniteľnosť CVE-2025-53799 v súčasti **Windows Imaging Component** môže neautorizovaný lokálny útočník zneužiť na **získanie citlivých informácií** z častí haldy. Zraniteľnosť spočíva v možnosti použitia neinicializovaných zdrojov a útočník na jej zneužitie potrebuje presvedčiť obeť, aby otvorila škodlivý súbor.

Kritická zraniteľnosť s identifikátorom CVE-2025-54918 v komponente súčasti **Windows NTLM** spočíva v nesprávnej implementácii autentifikačných mechanizmov. Vzdialený útočník s nízkymi oprávneniami ju môže zneužiť na **zvýšenie svojich oprávnení** na úroveň **SYSTEM**. Útočník nepotrebuje interakciu obete.

Kritická zraniteľnosť s identifikátorom CVE-2025-55224 vo virtualizačnej platforme **Windows Hyper-V** dovoľuje po výhre súbehu v komponente **Win32K – GRFX** použiť dealokované miesto v pamäti. Útočník s nízkymi oprávneniami v hosťovskom systéme ju môže zneužiť na **vykonanie ľubovoľného kódu** v hostiteľskom systéme. Útočník s prístupom ku virtuálnemu stroju nepotrebuje interakciu obete. Ak takýto prístup nemá, môže presvedčiť obeť, aby otvorila škodlivý súbor v hosťovskom stroji.

Súčasť **Windows Graphics Component** obsahuje kritické zraniteľnosti s identifikátorom CVE-2025-53800 a CVE-2025-55228. Súvisia s nesprávnou inicializáciou zdrojov a možnosťou použitia dealokovaného miesta v pamäti po výhre súbehu. Lokálny útočník s nízkymi oprávneniami ich môže zneužiť na **navýšenie svojich oprávnení** na úroveň **SYSTEM** a po výhre súbehu v komponente **Win32K – GRFX vykonanie ľubovoľného kódu**. Útočník s prístupom ku systému nepotrebuje interakciu obete. Ak takýto prístup nemá, môže presvedčiť obeť, aby otvorila škodlivý súbor.

Kritické zraniteľnosti s identifikátorom CVE-2025-55226 a CVE-2025-55236 v súčasti **Graphics Kernel** spočívajú v súbehu procesov kvôli nedostatočnej synchronizácii vykonávania a súbehu typu TOCTOU v spojení so zámenou typu premennej. Autentifikovaný útočník s nízkymi oprávneniami ich môže zneužiť na lokálne **vykonanie ľubovoľného kódu** zneužitím ním kontrolovaných vstupov.

Vysoko závažné zraniteľnosti CVE-2025-54101, CVE-2025-54106, CVE-2025-54113, CVE-2025-54916 a CVE-2025-54919 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 a obídenie bezpečnostných prvkov.

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 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-2025-53799
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53800
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-54918
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-55224
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-55226
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-55228
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-55236

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 september bezpečnostné aktualizácie, ktoré opravujú 3 kritických a 17 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritickú zraniteľnosť CVE-2025-53799 v súčasti **Windows Imaging Component** môže neautorizovaný lokálny útočník zneužiť na **získanie citlivých informácií** z častí haldy. Zraniteľnosť spočíva v možnosti použitia neinicializovaných zdrojov a útočník na jej zneužitie potrebuje presvedčiť obeť, aby otvorila škodlivý súbor.

Kritická zraniteľnosť **Microsoft Office** s označením CVE-2025-54910 súvisí s pretečením zásobníka na halde. Neautorizovaný útočník ich môže zneužiť na lokálne **vykonanie ľubovoľného škodlivého kódu**. Nepotrebuje na to interakciu obete. Pre jej zneužitie môže slúžiť aj vygenerovanie náhľadu súboru (Preview Pane).

Kritická zraniteľnosť CVE-2025-55242 sa nachádza v platforme **xBox Gaming Services**. Súvisí s nedostatočnou ochranou citlivých informácií. Neautorizovaný vzdialený útočník môže jej zneužitím získať **prístup k citlivým informáciám**. Potrebuje k tomu interakciu obete, ak útočník môže nahrať špeciálne vytvorené dokumenty s metasúbormi. Spoločnosť Microsoft zraniteľnosť opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre jej odstránenie.

Vysoko závažné zraniteľnosti spočívajú v pretečení medzipamäte na halde, nezabezpečenom ukladaní citlivých informácií, možnosti čítania medzipamäte mimo povolené hodnoty, použití dealokovaného miesta v pamäti, nedostatočnej ochrany súborových ciest, deserializácii nedôveryhodných dát a dereferencii nedôveryhodného ukazovateľa. Predmetné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu, získanie citlivých informácií, eskaláciu privilégií, obídenie bezpečnostných prvkov** a **spoofingové útoky**.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- 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 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 OfficePLUS
- Microsoft PC Manager
- Microsoft PowerPoint 2016 (32-bit edition)
- Microsoft PowerPoint 2016 (64-bit edition)
- 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
- Xbox Gaming Services

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-2025-53799
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-54910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-55242

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 september opravila jednu vysoko závažnú zraniteľnosť vo webovom prehliadači Microsoft Edge.

Vysoko závažná zraniteľnosť s identifikátorom CVE-2025-59521 spočíva v zámene typu premennej a umožňuje neautentifikovanému útočníkovi vzdialene vykonávať kód. Zneužitie zraniteľnosti vyžaduje interakciu zo strany obete, ktorá musí kliknúť na špeciálne vytvorený URL

odkaz. Útočník môže tiež získať prístup k citlivým informáciám a ovplyvniť dostupnosť v rámci karty prehliadača.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft Edge (Chromium-based) verzie staršie ako 140.0.3485.81

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-2025-59251

MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci september opravila 5 vysoko závažných zraniteľností v línii internetových prehliadačov Firefox a Firefox ESR.

Línie Firefox a Firefox ESR obsahujú zraniteľnosti CVE-2025-10527 a CVE-2025-10528 súvisiacu s neplatným ukazovateľom a možnosťou použitia dealokovanej pamäte v komponente Canvas2D v Graphics. Útočník jej zneužitím môže dosiahnuť **únik zo sandboxu**.

Zraniteľnosť CVE-2025-11152 v línii Firefox súvisí s pretečením celočíselnej premennej v komponente Canvas2D v Graphics. Útočník jej zneužitím môže dosiahnuť **únik zo sandboxu**.

Zraniteľnosť CVE-2025-11153 v komponente JIT nástroja JavaScript Engine v línii Firefox môže viesť k **miskompilácii JIT**.

Identifikátor CVE-2025-10537 pokrývajú sadu zraniteľností v líniách Firefox a Firefox ESR, ktoré ovplyvňujú bezpečnosť pamäte a môžu viesť ku **poškodeniu pamäte** alebo možnosti **vykonávať kód**.

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox a Firefox pre iOS verzie staršie ako 142

- Mozilla Firefox ESR verzie staršej ako 140.2

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 143.0.3 a Firefox ESR na verziu 140.3.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-73/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-75/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-80/

GOOGLE CHROME

V mesiaci september spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 1 kritickú a 11 vysoko závažných zraniteľností.

Kritická CVE-2025-10200 sa nachádza v komponente Serviceworker. Umožňuje použitie dealokovaného miesta v pamäti.

Komponent V8 obsahuje viacero vysoko závažných zraniteľností. CVE-2025-9864 dovoľuje použiť dealokované miesto v pamäti. CVE-2025-10891 a CVE-2025-10892 sú zapríčinené pretečením celočíselnej premennej a CVE-2025-10585 zámenou typu premennej. Zraniteľnosť CVE-2025-10890 súvisí s únikom informácií bočným kanálom.

Vysoko závažná zraniteľnosť CVE-2025-11205 v komponente WebGPU súvisí s pretečením zásobníka na halde. Rovnaký typ zraniteľnosti obsahuje aj komponent Video (CVE-2025-11206) a ANGLE (CVE-2025-10502).

Komponenty Dawn a WebRTC obsahujú vysoko závažné zraniteľnosti, ktoré dovoľujú použiť dealokované miesto v pamäti. Boli im priradené identifikátory CVE-2025-10500 a CVE-2025-10501.

Vysoko závažná zraniteľnosť CVE-2025-10201 v komponente Mojo vyplýva z nevhodnej implementácie nešpecifikovaných prvkov.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows a Mac verzie staršej ako 141.0.7390.54/55

- Google Chrome pre Linux verzie staršej ako 141.0.7390.54

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 141.0.7390.54/55 a Linux verzie aspoň na verziu 141.0.7390.54.

ZDROJE:

- https://chromereleases.googleblog.com/2025/09
- https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_9.html
- https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_17.html
- https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_23.html
- https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_25.html
- https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_30.html

4. ADOBE ACROBAT A READER

V mesiaci september spoločnosť Adobe opravila 1 kritickú zraniteľnosť v produktoch Adobe Acrobat a Reader.

Kritická zraniteľnosť CVE-2025-54257 spočíva v použití dealokovaného miesta v pamäti a možno ju zneužiť na vykonanie ľubovoľného kódu.

ZRANITEĽNÉ SYSTÉMY:

- Acrobat DC a Acrobat Reader DC verzie 25.001.20672 pre Windows a verzie 25.001.20668 pre Mac, a staršie
- Acrobat 2020 a Acrobat Reader 2020 pre Windows a Mac verzie 20.005.30774 a staršie
- Acrobat 2024 pre Windows a Mac verzie 24.001.30254 a staršie

ODPORÚČANIA:

Odporúčame aktualizáciu aspoň na verziu:

- Acrobat DC a Acrobat Reader DC pre Windows a Mac 25.001.20693
- Acrobat 2020 a Acrobat Reader 2020 pre Windows 20.005.30793 a Mac 20.005.30791
- Acrobat 2024 pre Windows a Mac 24.001.30264

ZDROJE:

- https://helpx.adobe.com/security/security-bulletin.html#acrobat
- https://helpx.adobe.com/security/products/acrobat/apsb25-85.html

5. FRAMEWORKY

MICROSOFT .NET FRAMEWORK

V mesiaci september 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 21. októbra 2025.

ZDROJE:

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

INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

ZERO-DAY ZRANITEĽNOSŤ VO FREEPBX BOLA OPRAVENÁ

Bezpečnostní výskumníci zo Sangoma FreePBX Security Team informovali o kritickej zero-day zraniteľnosti v rozšírenom open-source komunikačnom softvéri FreePBX, využívanom najmä v call centrách. Zraniteľnosť bola označená ako aktívne zneužívaná. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V OPERAČNOM SYSTÉME FIREWALLOV WATCHGUARD FIREBOX

Spoločnosť WatchGuard vydala bezpečnostné aktualizácie svojich firewallov Firebox, ktoré opravujú kritickú zraniteľnosť operačného systému Fireware OS. CVE-2025-9242 by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V PLATFORME PRE PRENOS SÚBOROV FORTRA GOANYWHERE MFT

Spoločnosť Fortra vydala bezpečnostné aktualizácie webového nástroja pre prenos súborov GoAnywhere MFT (Managed File Transfer), ktoré opravujú kritickú zraniteľnosť. CVE-2025-10035 by vzdialený neautentifikovaný útočník mohol zneužiť na injekciu príkazov a získanie úplnej kontroly nad systémom. Zraniteľnosť je aktívne zneužívaná. Viac informácií na stránke.

KOMPROMITOVANÉ BALÍČKY V KNIŽNICI NPM ŠÍRIA MALVÉR

Bezpečnostní výskumníci odhalili nový útok na dodávateľský reťazec v npm registri, ktorý zasiahol stovky balíčkov od rôznych udržiavateľov. Tieto balíčky sa používajú ako súčasti softvéru a webových stránok, od komerčných aplikácií až po open-source projekty, čo znamená, že počet ohrozených produktov nie je možné presne určiť. Viac informácií na stránke.

CISCO V SÚVISLOSTI SO ZERO-DAY ZRANITEĽNOSŤAMI ODPORÚČA BEZODKLADNÚ AKTUALIZÁCIU FIREWALLOV ASA A FTD

Spoločnosť CISCO vydala bezpečnostné aktualizácie, ktoré okrem iného opravujú dve aktívne zneužívané zero-day zraniteľnosti vo firewalloch ASA (Adaptive Security Appliance) a FTD (Firewall Threat Defense). CVE-2025-20362 možno zneužiť na obídenie mechanizmov autentifikácie a CVE-2025-20333 na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.