MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

MÁJ 2025

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci máj 3 kritické a 41 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritická zraniteľnosť CVE-2025-29833 sa nachádza v komponente Microsoft Virtual Machine Bus VMBus a súvisí so súbehom procesov typu TOCTOU. Zraniteľnosť umožňuje **lokálne vykonanie kódu**. Neautentifikovaný útočník potrebuje pre zneužitie zraniteľnosti interakciu obete a vyhrať súbeh procesov. Útok môže ovplyvniť funkcionalitu hostiteľa Hyper-V.

Kritické zraniteľnosti s identifikátormi CVE-2025-29966 a CVE-2025-29967 v komponente **Windows Remote Desktop Client** spočívajú v pretečení vyrovnávacej pamäte na halde. To umožňuje neautorizovanému útočníkovi **vzdialené vykonanie kódu**. Útočník môže zraniteľnosť zneužiť tak, že presvedčí obeť so zraniteľnou verziou Remote Desktop Client, aby sa pripojila k jeho inštancii Remote Desktop Server.

Vysoko závažné zraniteľnosti vo **Windows Server 2016** (CVE-2025-29831, CVE-2025-29840, CVE-2025-29962, CVE-2025-30388), **Windows Server 2019** (CVE-2025-29969), **Windows Server 2025** (CVE-2025-29963), **Windows 10** (CVE-2025-30397) a **Windows 11** (CVE-2025-29964) 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:

- Remote Desktop client for Windows Desktop
- Windows 10 for 32-bit Systems
- Windows 10 for x64-based Systems
- Windows 10 HLK version 20H2

- Windows 10 HLK version 21H1
- Windows 10 HLK version 21H2
- Windows 10 HLK Version 22H2
- 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 HLK 22H2
- Windows 11 HLK 24H2
- 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 App Client for Windows Desktop
- Windows HLK for Windows 10 version 2004
- Windows HLK for Windows Server 2019
- Windows HLK for Windows Server 2025
- Windows HLK Version 1809
- 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-2025-29833
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29967
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29966

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.

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 máj bezpečnostné aktualizácie, ktoré opravujú 2 kritické a 17 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritické zraniteľnosti CVE-2025-30377 a CVE-2025-30386 v produktoch **Microsoft Office** súvisia s možnosťou použitia dealokovaného miesta v pamäti. Neautentifikovaný útočník ich môže zneužiť na **vykonanie ľubovoľného škodlivého kódu**. Nepotrebuje na to nevyhnutne presvedčiť obeť, aby si napríklad stiahla a otvorila špeciálne vytvorený súbor. Útok sa spustí napríklad aj po prijatí e-mailu prostredníctvom náhľadu súboru (Preview Pane).

Vysoko závažné zraniteľnosti spočívajú v možnosti čítania mimo povolených hodnôt v pamäti, pretečení medzipamäte na halde, použití odalokovaného miesta v pamäti, zámene typu premennej, dereferencii nedôveryhodného ukazovateľa, deserializácii nedôveryhodných dát, nedostatočnej ochrane citlivých dát a nevhodnej kontroly prístupov a oprávnení. Predmetné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu** a **eskaláciu privilégií**.

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 for Universal
- 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 PC Manager
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription 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-2025-30377
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30386

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 máj 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 máj opravila 3 kritické zraniteľnosti v línii internetových prehliadačov Firefox a Firefox ESR.

CVE-2025-4918 v línii Firefox a Firefox ESR umožňuje **čítať a zapisovať do pamäte mimo povolené hodnoty** pri spracovaní objektov JavaScript Promise.

CVE-2025-4919 v línii Firefox a Firefox ESR umožňuje **čítať a zapisovať do pamäte mimo povolené hodnoty** na objektoch JavaScript, kvôli zámene veľkosti indexov poľa.

Línie Firefox a Firefox ESR obsahujú tiež kritickú zraniteľnosť MFSA-TMP-2025-0001. Pri inicializácii enkódera WebRTC môže vo funkcii vpx_codec_enc_init_multi dôjsť ku chybnej alokácii pamäte a pokusu o dvojité uvoľnenie. To môže viesť ku **poškodeniu pamäte**, čo môže byť zneužité pre ďalšie útoky.

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox verzie staršie ako 139
- Mozilla Firefox ESR verzie staršej ako 115.24 a 128.11

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 139 a Firefox ESR na verziu 115.24 alebo 128.11.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-36/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-37/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-38/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-42/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-43/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-44/

GOOGLE CHROME

V mesiaci máj spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 4 vysoko závažné zraniteľnosti.

Komponent Loader obsahuje vysoko závažnú zraniteľnosť CVE-2025-4664, ktorá súvisí s nevhodnou implementáciou bezpečnostných politík.

Vysoko závažná zraniteľnosť CVE-2025-4609 v komponente Mojo vyplýva z nesprávneho narábania s nešpecifikovanými funkciami.

Vysoko závažná zraniteľnosť CVE-2025-5063 v komponente Compositing súvisí s možnosťou použitia dealokovaného miesta v pamäti. Útočník môže zneužiť poškodenie haldy pomocou špeciálne vytvorenej HTML stránky.

Zneužiť možnosť zápisu do pamäte mimo povolené hodnoty umožňuje vysoko závažná zraniteľnosť CVE-2025-5280 v komponente V8.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows a Mac verzie staršej ako 137.0.7151.55/56
- Google Chrome pre Linux verzie staršej ako 137.0.7151.55

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 137.0.7151.55/56 a Linux verzie aspoň na verziu 137.0.7151.55.

ZDROJE:

- https://chromereleases.googleblog.com/2025/05
- https://chromereleases.googleblog.com/2025/05/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2025/05/stable-channel-update-for-desktop_14.html
- https://chromereleases.googleblog.com/2025/05/stable-channel-update-for-desktop_27.html
- https://nvd.nist.gov/vuln/detail/CVE-2025-5063

4. ADOBE ACROBAT A READER

V mesiaci máj 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 máj spoločnosť Microsoft opravila 1 vysoko závažnú zraniteľnosť vo frameworku .NET.

Zraniteľnosť CVE-2025-26646 v .NET spočíva v možnosti manipulovať s cestou alebo názvom súborov pomocou používateľských vstupov. To umožňuje vzdialenému útočníkovi s nízkymi oprávneniami vykonávať na sieti útoky typu spoofing.

ZRANITEĽNÉ SYSTÉMY:

- .NET 8.0 pre Windows, Linux a MacOS
- .NET 9.0 pre Windows, Linux a MacOS

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-2025-26646

ORACLE JAVA

Spoločnosť Oracle plánuje vydať veľkú sadu opráv 15. júla 2025.

ZDROJE:

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

6. Iné závažné zraniteľnosti

Aktívne zneužívaná zraniteľnosť v SAP NetWeaver

Spoločnosť SAP vydala bezpečnostné aktualizácie svojho aplikačného servera SAP NetWeaver, ktoré opravujú kritickú zraniteľnosť. CVE-2025-31324 možno zneužiť na nahratie súborov, vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi na prienik do zraniteľných systémov. Viac informácií na stránke.

Aktívne zneužívané kritické zraniteľnosti v Craft CMS

Vývojári redakčného systému Craft CMS vydali bezpečnostné aktualizácie, ktoré opravujú dve aktívne zneužívané kritické zraniteľnosti. Kritické zraniteľnosti s označením CVE-2025-32432 a CVE-2024-58136 by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

Ďalšia aktívne zneužívaná zraniteľnosť SAP NetWeaver

Spoločnosť SAP vydala bezpečnostné aktualizácie pre opravu ďalšej kritickej zraniteľnosti s identifikátorom CVE-2025-42999, ktorá je aktívne zneužívaná v rámci útokov súvisiacich so zneužitím CVE-2025-31324. Viac informácií na stránke.

Kritická zraniteľnosť v IP kamerách Ubiquiti UniFi Protect

Spoločnosť Ubiquiti vydala bezpečnostné aktualizácie pre svoje IP kamery UniFi Protect, ktoré opravujú kritickú zraniteľnosť. Zraniteľnosť s identifikátorom CVE-2025-23123 možno zneužiť na vykonanie škodlivého kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

Zraniteľnosť webového manažmentového nástroja Webmin

Vývojári webového ovládacieho panelu pre vzdialený manažment serverov Webmin vydali aktualizáciu svojho produktu, ktorá opravuje vysoko závažnú zraniteľnosť. CVE-2025-2774 by vzdialený autentifikovaný útočník mohol zneužiť na eskaláciu privilégií, vykonanie ľubovoľného kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V NÁSTROJI PRE MANAŽMENT OVLÁDAČOV ASUS DRIVERHUB

Spoločnosť ASUS vydala bezpečnostné aktualizácie svojho nástroja pre manažment ovládačov ASUS DriverHub, ktoré opravujú dve zraniteľnosti, z čoho jedna je označená ako kritická. Vzdialený neautentifikovaný útočník by zreťazením zraniteľností s identifikátormi CVE-2025-3462 a CVE-2025-3463 mohol vzdialene vykonať škodlivý kód a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V BEZDRÔTOVÝCH KONTROLÉROCH CISCO

Spoločnosť Cisco vydala bezpečnostné aktualizácie pre svoje bezdrôtové kontroléry s operačným systémom Cisco IOS XE, ktoré opravujú kritickú zraniteľnosť. CVE-2025-20188 by vzdialený útočník mohol zneužiť na nahratie súborov, vzdialené vykonanie príkazov s oprávneniami používateľa root a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ VO VIZUALIZAČNEJ PLATFORME KIBANA

Spoločnosť Elastic vydala bezpečnostné aktualizácie svojej vizualizačnej platformy Kibana, ktoré opravujú kritickú zraniteľnosť. CVE-2025-25014 by vzdialený autentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

KRITICKÁ ZERO-DAY ZRANITEĽNOSŤ V PRODUKTOCH FORTINET FORTIVOICE, FORTIMAIL, FORTINDR, FORTIRECORDER A FORTICAMERA

Spoločnosť Fortinet vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zero-day zraniteľnosť v produktoch FortiVoice, FortiMail, FortiNDR, FortiRecorder a FortiCamera. CVE-2023-32756 možno zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Zraniteľnosť je aktívne zneužívaná v rámci útokov na telefónne systémy FortiVoice. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÉ ZRANITEĽNOSTI V PRODUKTOCH IVANTI EPMM A NEURONS FOR ITSM

Spoločnosť Ivanti vydala bezpečnostné aktualizácie pre kritickú zraniteľnosť produktu Neurons for ITSM a dve aktívne zneužívané zraniteľnosti v Endpoint Manager Mobile (EPMM). Zraniteľnosti s identifikátormi CVE-2025-22462, CVE-2025-4427 a CVE-2025-4427 možno zneužiť na získanie neoprávneného prístupu k citlivým údajom, vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

ZRANITEĽNOSTI FRAPPE FRAMEWORK

Stručný prehľad pythonovského frameworku Frappe, ktorý vykonali výskumníci CSIRT.SK, odhalil množstvo zraniteľností umožňujúcich útočníkom vykonávať rôzne druhy útokov. V základni kódu sa môže nachádzať množstvo ďalších chýb, ktoré len čakajú na objavenie. Viac informácií na stránke.