MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

AUGUST 2025

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci august 6 kritických a 63 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritickú zraniteľnosť CVE-2025-48807 v komponente **Windows Hyper-V** môže neautorizovaný lokálny útočník zneužiť na **vykonanie ľubovoľného kódu**. Zraniteľnosť spočíva v nevhodnej kontrole komunikačných kanáloch na koncové body v Hyper-V a útočník na jej zneužitie potrebuje vystihnúť nešpecifikovanú aktivitu od administrátora na hostiteľskom systéme.

Kritická zraniteľnosť s identifikátorom CVE-2025-50165 v súčasti **Windows Graphics Component** spočíva v dereferencii nedôveryhodného ukazovateľa. Neautorizovaný vzdialený útočník ju môže zneužiť na **vykonanie ľubovoľného kódu**. Útočník nepotrebuje interakciu obete a zraniteľnosť môže aktivovať podvrhnutím škodlivého obrázku vo formáte JPEG, napríklad v dokumente MS Office, alebo inom.

Kritická zraniteľnosť s identifikátorom CVE-2025-50176 v súčasti **DirectX Graphics Kernel** spočíva v zámene typu premennej pri prístupe ku zdrojom a pretečení zásobníka haldy. Autentifikovaný útočník s nízkymi oprávneniami ju môže zneužiť na lokálne **vykonanie ľubovoľného kódu**.

Komponent **Microsoft Message Queuing (MSMQ)** obsahuje chybu umožňujúcu použitie dealokovaného miesta v pamäte. Zraniteľnosť s identifikátorom CVE-2025-50177 dovoľuje neautorizovanému útočníkovi **vzdialené vykonanie kódu** na zraniteľnom systéme. Pre jej zneužitie potrebuje útočník poslať v rýchlom slede sériu paketov MSMQ cez http serveru a vyhrať súbeh procesov.

Kritická zraniteľnosť CVE-2025-53766 sa nachádza v komponente **Windows GDI+**. Súvisí pretečením zásobník na halde. Neautorizovaný vzdialený útočník ju môže zneužiť na **vykonanie ľubovoľného kódu** alebo môže získať **prístup k citlivým informáciám** o webových službách. Interakcia obete nie je nevyhnutná, ak útočník môže nahrať špeciálne vytvorené dokumenty s metasúbormi.

Zraniteľnosť CVE-2025-53778 vo **Windows NTLM** súvisí s nevhodnou implementáciou autentifikácie. Autorizovanému vzdialenému útočníkovi umožňuje **navýšiť svoje oprávnenia** na zraniteľnom systéme až na úroveň SYSTEM.

Vysoko závažné zraniteľnosti CVE-2025-49757, CVE-2025-50160, CVE-2025-50162, CVE-2025-50163, CVE-2025-50164, CVE-2025-50169, CVE-2025-53131, CVE-2025-53143, CVE-2025-53144, CVE-2025-53145, CVE-2025-53152, CVE-2025-53720 a CVE-2025-55231 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 spoofingové útoky.

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 Security App
- 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-2025-48807
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-50165
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-50176
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-50177
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53766
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53778

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 august bezpečnostné aktualizácie, ktoré opravujú 8 kritických a 14 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritické zraniteľnosti CVE-2025-53731 a CVE-2025-53740 v produktoch **Microsoft Office** súvisia s možnosťou použitia dealokovaného miesta v pamäti. Neautorizovaný útočník ich môže zneužiť na lokálne **vykonanie ľubovoľného škodlivého kódu**. Vektorom pre zneužitie chýb zabezpečenia môže byť aj vygenerovanie náhľadu súboru (Preview Pane).

Kritické zraniteľnosti **Microsoft Word** s označením CVE-2025-53733 a CVE-2025-53784 súvisia s nesprávnou konverziou typov číselných premenných a možnosťou použitia dealokovaného miesta v pamäti. Neautorizovaný útočník ich môže zneužiť na lokálne **vykonanie ľubovoľného škodlivého kódu**. Pre jej zneužitie môže slúžiť aj vygenerovanie náhľadu súboru (Preview Pane).

Kritická zraniteľnosť CVE-2025-53766 sa nachádza v komponente **Windows GDI+**. Súvisí pretečením zásobník na halde. Neautorizovaný vzdialený útočník ju môže zneužiť na **vykonanie ľubovoľného kódu** alebo môže získať **prístup k citlivým informáciám** o webových službách. Interakcia obete nie je nevyhnutná, ak útočník môže nahrať špeciálne vytvorené dokumenty s metasúbormi.

Kritické zraniteľnosti CVE-2025-53774 a CVE-2025-53787 v **Microsoft 365 Copilot BizChat** spočívajú v možnosti injektovať príkazy a môžu spôsobiť únik citlivých informácií. CVE-2025-

53795 v **Microsoft PC Manager** spočíva v nevhodne implementovanej autorizácii, čo dovoľuje vzdialenému neautorizovanému útočníkovi **získať vyššie oprávnenia**. Spoločnosť Microsoft zraniteľnosti opravila na svojich systémoch a nie je potrebné vykonať ďalšie aktivity pre ich odstránenie.

Vysoko závažné zraniteľnosti spočívajú v pretečení medzipamäte na halde, použití neinicializovaných zdrojov, možnosti čítania medzipamäte mimo povolené hodnoty, použití odalokovaného miesta v pamäti, zámene typu premennej, deserializácii nedôveryhodných dát a SSRF. Predmetné zraniteľnosti možno zneužiť na **vzdialené vykonanie škodlivého kódu, získanie citlivých informácií** a **eskaláciu privilégií**.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft 365 Copilot's Business Chat
- 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 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 Teams for Android
- Microsoft Teams for Desktop
- Microsoft Teams for iOS
- Microsoft Teams for Mac
- Microsoft Word 2016 (32-bit edition)
- Microsoft Word 2016 (64-bit 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-2025-53731
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53733
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53740
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53766
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53774
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53784
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53787
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53795

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 august 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 august opravila 6 vysoko závažných zraniteľností v línii internetových prehliadačov Firefox a Firefox ESR.

Línie Firefox a Firefox ESR obsahujú zraniteľnosť CVE-2025-9179 súvisiacu s neplatným ukazovateľom v komponente GMP, ktorý spracúva šifrované multimediálne dáta. Útočník jej zneužitím môže spôsobiť poškodenie pamäte a **uniknúť zo sandboxu**.

Zraniteľnosť CVE-2025-9180 v líniách Firefox a Firefox ESR môže zapríčiniť **obídenie politiky „same-origin“**. Chyba sa nachádza v komponente Canvas2D v Graphics.

Kritická zraniteľnosť CVE-2025-55030 v línii Firefox pre iOS môže zapríčiniť nežiadané vykreslenie súborov niektorých typov MIME (Attachment) namiesto ich stiahnutia, čo by umožnilo **útoky typu XSS**. Chyba súvisí s nežiadaným ignorovaním hlavičiek Content-Disposition.

Identifikátory CVE-2025-9184 a CVE-2025-9185 pokrývajú sadu zraniteľností v líniách Firefox a Firefox ESR a CVE-2025-9187 vo Firefox, 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 115.27, 128.14 a 140.2

ODPORÚČANIA:

Odporúčame aktualizovať Firefox a Firefox pre iOS na verziu 142, Firefox ESR na verziu 115.27, 128.14 alebo 140.2.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-64/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-65/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-66/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-67/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-68/

GOOGLE CHROME

V mesiaci august spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 1 kritickú a 4 vysoko závažné zraniteľnosti.

Kritická CVE-2025-9478 a vysoko závažná zraniteľnosť CVE-2025-8901 sa nachádzajú v komponente ANGLE. Prvá umožňuje použitie dealokovaného miesta v pamäti, druhá zápis do pamäte mimo povolené hodnoty.

Vysoko závažná zraniteľnosť CVE-2025-8880 v komponente V8 súvisí so vznikom zneužiteľného súbehu procesov. Tento komponent obsahuje tiež zraniteľnosť CVE-2025-9132, ktorá dovoľuje zapisovať do pamäte mimo povolené hodnoty.

Vysoko závažná zraniteľnosť CVE-2025-8879 v komponente libaom súvisí s pretečením zásobníka na halde.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows a Mac verzie staršej ako 139.0.7258.154/.155

- Google Chrome pre Linux verzie staršej ako 139.0.7258.154

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 139.0.7258.154/.155 a Linux verzie aspoň na verziu 139.0.7258.154.

ZDROJE:

- https://chromereleases.googleblog.com/2025/08
- https://chromereleases.googleblog.com/2025/08/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2025/08/stable-channel-update-for-desktop_12.html
- https://chromereleases.googleblog.com/2025/08/stable-channel-update-for-desktop_19.html
- https://chromereleases.googleblog.com/2025/08/stable-channel-update-for-desktop_26.html

4. ADOBE ACROBAT A READER

V mesiaci august 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 august 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

KRITICKÁ AKTÍVNE ZNEUŽÍVANÁ ZRANITEĽNOSŤ VO WORDPRESS DOPLNKU ALONE

WordPress webstránky využívajúce tému menom Alone, sú aktívne zneužívané na vzdialené vykonávanie škodlivého kódu cez kritickú zraniteľnosť. Toto zneužitie bolo detegované už vo viac ako 120 tisíc prípadoch. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V JAVASCRIPT BALÍČKU NODE-SAML

Vývojári knižnice Node-SAML vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje kritickú bezpečnostnú zraniteľnosť vo verifikáci kryptografických podpisov, čo môže spôsobiť neautorizovaný prístup k citlivým údajom. Viac informácií na stránke.

GOOGLE OPRAVIL AKTÍVNE ZNEUŽÍVANÉ ZRANITEĽNOSTI OPERAČNÉHO SYSTÉMU ANDROID

Spoločnosť Google vydala bezpečnostné aktualizácie pre svoj operačný systém Andorid, ktoré opravujú 6 zraniteľností, z čoho 1 je označená ako kritická a 2 ako aktívne zneužívané. Aktívne zneužívané CVE-2025-21479 a CVE-2025-27038 v komponentoch Qualcomm možno zneužiť na poškodenie obsahu pamäte. Viac informácií na stránke.

VYSOKO ZÁVAŽNÁ ZRANITEĽNOSŤ V CURSOR AI IDE

Vývojári AI editora kódu Cursor vydali bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť. CVE-2025-54136 možno zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

ZERO-DAY ZRANITEĽNOSTI V PRODUKTE ADOBE EXPERIENCE MANAGER FORMS ON JEE

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoj produkt Adobe Experience Manager (AEM) Forms on JEE, ktoré opravujú dve kritické zero-day zraniteľnosti. Zraniteľnosti možno zneužiť na získanie neoprávneného prístupu k citlivým údajom, vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

MICROSOFT VYDAL USMERNENIE K ZÁVAŽNEJ ZRANITEĽNOSTI V HYBRIDNÝCH NASADENIACH MS EXCHANGE

poločnosť Microsoft vydala usmernenie pre mitigáciu bezpečnostnej zraniteľnosti CVE-2025-53786 s vysokou závažnosťou pre svoj produkt MS Exchange. Zatiaľ nebolo detegované aktívne zneužívanie zraniteľnosti, avšak Microsoft varuje, že zneužitie je ťažko detekovateľné. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V KAMERÁCH OD AXIS COMMUNICATIONS DOVOĽUJE VZDIALENÉ VYKONÁVANIE KÓDU

Bezpečnostní výskumníci z Claroty Team82 zverejnili informácie o zraniteľnostiach produktov spoločnosti Axis Communications z ktorých jedna CVE-2025-30023 je kritická a môže byť použitá na útok na serverovú aj klientskú stranu nasadených produktov. Viac informácií na stránke.

AKTUALIZÁCIA NÁSTROJA WINRAR OPRAVILA AKTÍVNE ZNEUŽÍVANÚ ZERO-DAY ZRANITEĽNOSŤ

Vývojári archivačného nástroja WinRAR vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje závažnú bezpečnostnú zraniteľnosť CVE-2025-8088. Táto zraniteľnosť je často zneužívaná vo phishingových kampaniach na distribúciu škodlivého kódu. Viac informácií na stránke.

WIN-DDOS: NOVÁ TECHNIKA DISTRIBUOVANÉHO NARUŠENIA DOSTUPNOSTI SLUŽBY

Bezpečnostní výskumníci zverejnili na stretnutí DEF CON 33 informácie o zraniteľnosti CVE-2025-32724, ktorá ohrozuje verejne dostupné doménové radiče dosiahnuteľné z internetu. Tie sa vedia efektívne zmeniť na obete, a tiež botov vyvolávajúcich narušenie dostupnosti služby. Zraniteľnosť má povahu zero-click a dovoľuje útočníkovi spôsobiť narušenie služby bez nákladnej alebo špecializovanej sady nástrojov. Viac informácií na stránke.

XEROX VYDAL BEZPEČNOSTNÉ ZÁPLATY PRE VYSOKO ZÁVAŽNÉ ZRANITEĽNOSTI

Spoločnosť Xerox vydala urgentné bezpečnostné varovanie týkajúce sa dvoch kritických zraniteľností v softvéri FreeFlow Core. Tieto zraniteľnosti umožňujú útočníkom vykonať útoky Server-Side Request Forgery (SSRF) a vzdialene vykonávať kód. Viac informácií na stránke.

SAP V AUGUSTOVOM PATCH TUESDAY OPRAVIL VIACERO KRITICKÝCH A VYSOKO ZÁVAŽNÝCH ZRANITEĽNOSTÍ VO VIACERÝCH PRODUKTOCH

Spoločnosť SAP vydala 12. augusta 2025 bezpečnostné aktualizácie obsahujúce opravy pre 20 zraniteľností. 3 z nich sú hodnotené ako kritické a umožňujú injektovanie kódu. 2 vysoko závažné dovoľujú získať vyššie oprávnenia, obchádzať autorizáciu a injektovať ABAP kód. Viac informácií na stránke.

ANALYTICI UPOZORŇUJÚ NA BEZPEČNOSTNÉ KAMERY DAHUA – MAJÚ 2 ZÁVAŽNÉ ZRANITEĽNOSTI

Bezpečnostní výskumníci z Bitdefender IoT Research Team zverejnili informácie o zraniteľnostiach CVE-2025-31700 a CVE-2025-31701 vo firmvéri pre bezpečnostné kamery značky Dahua. Ide o závažné zraniteľnosti, ktoré vie útočník zneužiť na vzdialené vykonávanie kódu. Viac informácií na stránke.

ZÁVAŽNÁ ZRANITEĽNOSŤ FORTIWEB UMOŽŇUJE OBÍSŤ AUTENTIFIKÁCIU

Spoločnosť Fortinet opravila vysoko závažnú zraniteľnosť vo svojich zariadeniach FortiWeb, ktorá z dôvodu nevhodnej validácie parametrov v cookies umožňuje vzdialeným útočníkom obísť autentifikáciu a získať administrátorské oprávnenia. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ CISCO SECURE FIREWALL MANAGEMENT CENTER DOVOĽUJE VYKONÁVAŤ SYSTÉMOVÉ PRÍKAZY

Spoločnosť Cisco opravila kritickú zraniteľnosť v Cisco Secure Firewall Management Center, ktorá z dôvodu nevhodnej validácie používateľských vstupov dovoľuje vzdialenému útočníkovi pri prihlasovaní odoslať požiadavku obsahujúcu príkaz Shell. Ten zraniteľné zariadenie vykoná. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ ZÁVAŽNÁ ZRANITEĽNOSŤ APPLE IOS, IPADOS A MACOS

Spoločnosť Apple opravila vysoko závažnú aktívne zneužívanú zraniteľnosť v komponente ImageIO systémov macOS, iOS a iPadOS, ktoré umožňuje útočníkom spôsobiť poškodenie pamäte, zneužiteľné na ďalšie fázy útoku. To nastáva pri spracovaní špeciálne upraveného obrázkového súboru. Viac informácií na stránke.

NOVÉ ZÁVAŽNÉ ZRANITEĽNOSTI CITRIX NETSCALER MÔŽU BYŤ AKTÍVNE ZNEUŽÍVANÉ

Spoločnosť Citrix opravila jednu kritickú a dve vysoko závažné zraniteľnosti zariadení NetScaler ADC a NetScaler Gateway. Kritická zraniteľnosť je pravdepodobne aktívne zneužívaná. Viac informácií na stránke.