MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

DECEMBER 2024

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci december 17 kritických a 42 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritická zraniteľnosť CVE-2024-49105 v **Remote Desktop Client** spočíva v nesprávnej implementácii mechanizmov riadenia prístupu a vzdialený útočník by ju mohol zneužiť na **vzdialené vykonanie kódu**. Zneužitie zraniteľnosti **vyžaduje interakciu** zo strany používateľa s oprávneniami administrátora, ktorý musí iniciovať RDP spojenie na škodlivý server pod kontrolou útočníka.

Zraniteľnosti v komponente **Windows Remote Desktop Services** spočívajú v použití odalokovaného miesta v pamäti a nedostatočnom zabezpečení citlivých údajov v pamäti (CVE-2024-49106, CVE-2024-49108, CVE-2024-49115, CVE-2024-49116, CVE-2024-49123, CVE-2024-49128, CVE-2024-49132), nesprávnom vyhodnocovaní dátových typov (CVE-2024-49119) a nesprávnej inicializácii premenných (CVE-2024-49120) a umožňujú **vzdialené vykonanie kódu**. Zraniteľnosti možno zneužiť pripojením sa na zraniteľné systémy v konfigurácii Remote Desktop Gateway. Úspešné zneužitie zraniteľností vyžaduje, aby útočník vyhral súbeh procesov.

Komponent **Windows Lightweight Directory Access Protocol (LDAP)** obsahuje kritickú zraniteľnosť s označením CVE-2024-49112, ktorú by vzdialený neautentifikovaný útočník prostredníctvom **špeciálne vytvorených volaní LDAP** mohol zneužiť na **vzdialené vykonanie kódu**. Pokusy o zneužitie zraniteľnosti je možné mitigovať aj blokovaním prichádzajúcich volaní RPC z nedôveryhodných sietí v nastaveniach doménového radiča.

Zraniteľnosti CVE-2024-49124 a CVE-2024-49127 v **Windows Lightweight Directory Access Protocol (LDAP)** spočívajú v použití odalokovaného miesta v pamäti a v nesprávnej synchronizácii procesov pri prístupe ku zdieľaným zdrojom. Vzdialený neautentifikovaný útočník by ju zaslaním špeciálne vytvorených požiadaviek mohol zneužiť na **vzdialené vykonanie kódu** s oprávneniami používateľa SYSTEM. Zneužitie zraniteľnosti vyžaduje, aby útočník vyhral súbeh procesov.

Zraniteľnosť v hypervízore **Hyper-V** (CVE-2024-49117) spočíva v generovaní nesprávnych stavových kódov a možno ju zneužiť na **vzdialené vykonanie kódu** na hostiteľskom serveri. Zneužitie zraniteľnosti vyžaduje, aby autentifikovaný útočník z virtuálneho stroja (VM) zaslal špeciálne vytvorenú požiadavku pre manipuláciu so súbormi na hardvérové zdroje VM. Úspešné

zneužitie zraniteľnosti môže viesť k tzv. **cross-VM útoku**, v rámci ktorého na hostiteľskom zariadení dochádza ku kompromitácii viacerých virtuálnych strojov.

Zraniteľnosti v komponente **Microsoft Message Queuing (MSMQ)** spočívajú v použití odalokovaného miesta v pamäti a umožňujú **vzdialené vykonanie kódu**. Zraniteľnosti je možné zneužiť **zaslaním špeciálne vytvorených MSMQ paketov** na MSMQ server. Úspešné zneužitie zraniteľnosti CVE-2024-49122 a CVE-2024-49118 je časovo náročné, nakoľko vyžaduje, aby útočník vyhral súbeh procesov.

Windows **Local Security Authority Subsystem Service (LSASS)** obsahuje zraniteľnosť CVE-2024-49126 spočívajúcu v použití odalokovaného miesta v pamäti a nedostatočnom zabezpečení citlivých údajov v pamäti. Vzdialený neautentifikovaný útočník by ju prostredníctvom špeciálnych sieťových volaní mohol zneužiť na **vzdialené vykonanie kódu**. Úspešné zneužitie zraniteľnosti vyžaduje, aby útočník vyhral súbeh procesov.

Vysoko závažné zraniteľnosti v komponentoch Input Method Editor (IME) (CVE-2024-49079), **Windows IP Routing Management Snapin** (CVE-2024-49080), **Windows Routing and Remote Access Service (RRAS)** (CVE-2024-49085, CVE-2024-49086, CVE-2024-49089, CVE-2024-49102, CVE-2024-49104, CVE-2024-49125), **Windows Domain Name Service** (CVE-2024-49091), by vzdialený útočník mohol zneužiť na **vzdialené vykonanie kódu** a úplné narušenie dôvernosti, integrity a dostupnosti systému. Zneužitie všetkých zraniteľností okrem CVE-2024-49080, CVE-2024-49089 a CVE-2024-49091 vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť škodlivý súbor alebo zaslať požiadavku na škodlivý server.

Ostatné zraniteľnosti vysokej závažnosti možno zneužiť na vzdialené vykonanie kódu, eskaláciu privilégií, zneprístupnenie služby alebo získanie neoprávneného prístupu k citlivým údajom.

ZRANITEĽNÉ SYSTÉMY:

- Remote Desktop client for Windows Desktop
- 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 10 for 32-bit Systems
- Windows 10 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 App Client for Windows Desktop
- 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-2024-49105
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49106
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49108
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49112
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49115
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49116

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49117
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49118
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49119
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49120
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49122
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49123
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49124
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49126
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49127
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49128
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49132

Koniec podpory pre Windows Server 2012 a Windows Server 2012 R2

Spoločnosť Microsoft plánovane zrušila podporu pre Windows Server 2012 a Windows Server 2012 R2. Po dátume 10. októbra 2023 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 systémov Windows Server 2012 a Windows Server 2012 R2 odporúčame prejsť na novšiu verziu operačného systému alebo používať rozšírenie ESU na dobu určitú. **Viac informácií na stránke.**

2. KANCELÁRSKE BALÍKY MICROSOFT OFFICE A OFFICE WEB APPS

Spoločnosť Microsoft vydala v mesiaci december bezpečnostné aktualizácie, ktoré opravujú 1 kritickú a 9 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritická zraniteľnosť vo webovej stránke **Microsoft Update Catalog** (CVE-2024-49147) spočíva v deserializácii nedôveryhodných dát a vzdialený neautentifikovaný útočník by ju mohol zneužiť na **eskaláciu privilégií** na webovom serveri. Zraniteľnosť bola automaticky opravená spoločnosťou Microsoft a nevyžaduje dodatočnú aktualizáciu systémov.

CVE-2024-49069 v produkte **Microsoft Excel** spočíva použití odalokovaného miesta v pamäti a vzdialený neautentifikovaný útočník by ju podvrhnutím špeciálne vytvorených súborov mohol zneužiť na **vzdialené vykonanie škodlivého kódu**. Zneužitie zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť škodlivé súbory.

Zraniteľnosti v **Microsoft Office** spočívajúce v nesprávnom riadení prístupov (CVE-2024-43600) a nesprávnom preklade odkazov pred prístupom k súborom (CVE-2024-49059) by lokálny autentifikovaný útočník mohol zneužiť na **eskaláciu privilégií** na úroveň oprávnení SYSTEM. Čítanie mimo povolených hodnôt v rámci CVE-2024-49065 by vzdialený neautentifikovaný útočník mohol zneužiť na **vzdialené vykonanie kódu**. Zneužitie tejto zraniteľnosti vyžaduje interakciu zo strany používateľa, ktorý musí kliknúť na priložený súbor a vyvolať zobrazenie jeho náhľadu.

Produkt **Microsoft SharePoint** obsahuje 4 vysoko závažné zraniteľnosti. Nesprávne riadenie prístupu (CVE-2024-49068) by vzdialený útočník mohol zneužiť na **eskaláciu privilégií**. Zraniteľnosť s označením CVE-2024-49070 spočívajúca v deserializácii nedôveryhodných dát umožňuje **vykonanie kódu**. CVE-2024-49062 a CVE-2024-49064 možno zneužiť na **získanie neoprávneného prístupu k citlivým údajom**. Zneužitie zraniteľnosti CVE-2024-49064 vyžaduje interakciu zo strany používateľa, ktorý musí kliknúť na špeciálne vytvorený URL odkaz.

Použitie odalokovaného miesta v pamäti v rámci **Microsoft Access** možno zneužiť na **vzdialené vykonanie kódu**. Zneužitie zraniteľnosti CVE-2024-49142 vyžaduje interakciu zo strany používateľa, ktorý musí stiahnuť a otvoriť špeciálne vytvorený súbor.

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 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 Server 2019
- Microsoft SharePoint Server Subscription Edition
- Microsoft Update Catalog
- Microsoft Word 2016 (32-bit edition)
- Microsoft Word 2016 (64-bit edition)

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-2024-49147
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43600
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49059

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49062
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49064
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49065
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49068
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49069
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49070
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49142

3. INTERNETOVÉ PREHLIADAČE

MICROSOFT INTERNET EXPLORER

Spoločnosť Microsoft ukončila podporu prehliadača Internet Explorer 15.6.2022 pre hlavnú líniu operačných systémov Windows 10 a 11. Spoločnosť Microsoft za mesiac december neopravila žiadne kritické ani vysoko závažné zraniteľnosti pre zvyšné operačné systémy podporujúce Internet Explorer.

ODPORÚČANIA:

Odporúčame prestať používať a odinštalovať Internet Explorer a nahradiť ho podporovaným prehliadačom Microsoft Edge.

ZDROJE:

- https://msrc.microsoft.com/update-guide/en-us

MICROSOFT EDGE

Spoločnosť Microsoft v mesiaci december neopravila žiadne kritické ani vysoko závažné zraniteľnosti vo webovom prehliadači Microsoft Edge.

ZDROJE:

- https://msrc.microsoft.com/update-guide/en-us

MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci december neopravila žiadne kritické ani vysoko závažné zraniteľnosti v línii internetových prehliadačov Firefox a Firefox ESR.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/

GOOGLE CHROME

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

Zraniteľnosti v komponente **V8** spočívajú v nesprávnom overovaní dátových typov (CVE-2024-12053, CVE-2024-12381, CVE-2024-12692, CVE-2024-12693 a CVE-2024-12695) a čítaní (CVE-2024-12693) a zápise (CVE-2024-12695) mimo povolených hodnôt v pamäti. Vzdialený neautentifikovaný útočník by ich mohol zneužiť na **vzdialené vykonanie kódu**.

Zraniteľnosti v komponentoch **Translate** (CVE-2024-12382) a **Compositing** (CVE-2024-12694) spočívajú v znovupoužití odalokovaného miesta v pamäti a možno ich zneužiť na **vzdialené vykonanie kódu**.

Zneužitie všetkých vyššie uvedených zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť špeciálne vytvorený webový obsah.

ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows a Mac verzie staršej ako 131.0.6778.204/.205
- Google Chrome pre Linux verzie staršej ako 131.0.6778.204

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 131.0.6778.204/.205 a Linux verzie aspoň na verziu 131.0.6778.204.

ZDROJE:

- https://chromereleases.googleblog.com/2024

- https://chromereleases.googleblog.com/2024/12/stable-channel-update-for-desktop.html
- https://chromereleases.googleblog.com/2024/12/stable-channel-update-for-desktop_10.html
- https://chromereleases.googleblog.com/2024/12/stable-channel-update-for-desktop_18.html
- https://exchange.xforce.ibmcloud.com/vulnerabilities/390604
- https://exchange.xforce.ibmcloud.com/vulnerabilities/391569
- https://exchange.xforce.ibmcloud.com/vulnerabilities/392706
- https://exchange.xforce.ibmcloud.com/vulnerabilities/392705
- https://exchange.xforce.ibmcloud.com/vulnerabilities/392703
- https://exchange.xforce.ibmcloud.com/vulnerabilities/391570
- https://exchange.xforce.ibmcloud.com/vulnerabilities/392704

4. ADOBE ACROBAT A READER

V mesiaci december spoločnosť Adobe opravila 2 kritické a 4 vysoko závažné zraniteľnosti v produktoch Adobe Acrobat a Reader.

Kritické zraniteľnosti spočívajúce v použití odalokovaného miesta v pamäti (CVE-2024-49530) a nesprávnej reštrikcii XML External Entity referencií (CVE-2024-49535) možno zneužiť na vykonanie škodlivého kódu.

Vysoko závažné zraniteľnosti s označením CVE-2024-49532, CVE-2024-49533 a CVE-2024-49534 spočívajú v čítaní mimo povolených hodnôt a možno ich zneužiť na získanie neoprávneného prístupu k citlivým údajom.

CVE-2024-49531 spočíva v dereferencii nulového ukazovateľa a možno ju zneužiť na zneprístupnenie služby.

Zneužitie vyššie uvedených zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí stiahnuť a otvoriť špeciálne vytvorené súbory.

ZRANITEĽNÉ SYSTÉMY:

- Acrobat DC a Acrobat Reader DC pre Windows a Mac verzie 24.005.20307 a staršie

- Acrobat 2020 a Acrobat Reader 2020 verzie 20.005.30730 pre Windows a verzie 20.005.30710 pre Mac a staršie
- Acrobat 2024 verzie 24.001.30213 pre Windows a verzie 24.001.30193 pre Mac a staršie

ODPORÚČANIA:

Odporúčame aktualizáciu aspoň na verziu:

- Acrobat DC a Acrobat Reader DC pre Windows a Mac 24.005.20320
- Acrobat 2020 a Acrobat Reader 2020 pre Windows a Mac 20.005.30748
- Acrobat 2024 pre Windows a Mac 24.001.30225

ZDROJE:

- https://helpx.adobe.com/security/products/acrobat/apsb24-92.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 21. januára 2025.

ZDROJE:

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

6. INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

KRITICKÉ ZRANITEĽNOSTI V MODULOCH WORDPRESS WPLMS A VIBEBP

Vývojári modulov WordPress WPLMS a VibeBP vydali bezpečnostné aktualizácie, ktoré opravujú 18 zraniteľností, z ktorých 7 je označených ako kritických. Kritické zraniteľnosti vo WPLMS možno zneužiť na nahranie súborov na server, vzdialené vykonanie kódu, eskaláciu privilégií a získanie úplnej kontroly nad systémom. Kritické zraniteľnosti vo VibeBP možno zneužiť na realizáciu SQL injekcie, eskaláciu privilégií z získanie úplnej kontroly nad systémom. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI VO FIREWALLOCH SOPHOS

Spoločnosť Sophos vydala bezpečnostné aktualizácie pre svoje firewally, ktoré opravujú tri zraniteľnosti, z ktorých dve sú označení ako kritické. CVE-2024-12727 a CVE-2024-12728 možno zneužiť na získanie neoprávneného prístupu do systému a vzdialené vykonanie kódu. Poslednú zraniteľnosť možno zneužiť na injekciu príkazov. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ ZRANITEĽNOSŤ V OPERAČNOM SYSTÉME PALO ALTO PAN-OS

Spoločnosť Palo Alto Networks vydala bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť v operačnom systéme PAN-OS. CVE-2024-3393 v komponente DNS Security možno zaslaním špeciálne vytvorených paketov zneužiť na zneprístupnenie služby a vyradenie firewallov. Zraniteľnosť súčasnosti aktívne zneužívajú útočníci. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V PRODUKTOCH APACHE MINA, HUGEGRAPH-SERVER A TRAFFIC CONTROL

Vývojári z The Apache Software Foundation vydali bezpečnostné aktualizácie, ktoré opravujú kritické zraniteľnosti v produktoch Apache. CVE-2024-52046 v sieťovom aplikačnom frameworku MINA možno zneužiť na vzdialené vykonanie škodlivého kódu. CVE-2024-43441 v Apache HugeGraph-Server umožňuje získanie úplnej kontroly nad systémom a CVE-2024-45387 (Traffic Control) možno zneužiť na realizáciu SQL injekcie. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V PRODUKTOCH ADOBE COLDFUSION

Spoločnosť Adobe vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť v produkte Adobe ColdFusion. CVE-2024-53961 možno zneužiť na získanie neoprávneného prístupu k citlivým údajom, ktoré možno následne zneužiť na realizáciu ďalších útokov a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ VO WEBOVÝCH SERVEROCH APACHE TOMCAT

Vývojári open-source webového servera Apache Tomcat vydali bezpečnostné aktualizácie opravujúce 2 zraniteľnosti, z ktorých jedna je označená ako kritická. CVE-2024-50379 by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ KRITICKÁ ZRANITEĽNOSŤ VO FRAMEWORKU APACHE STRUTS

Vývojári open-source frameworku pre tvorbu Java EE webových aplikácií Apache Struts vydali bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú kritickú zraniteľnosť. CVE-2024-53677 možno zneužiť na upload súborov a vzdialené vykonanie kódu. Na uvedenú zraniteľnosť je v súčasnosti dostupný proof-of-concept kód demonštrujúci postup jej zneužitia. Viac informácií na stránke.

KRITICKÉ BEZPEČNOSTNÉ ZRANITEĽNOSTI V PRODUKTOCH ADOBE

Spoločnosť Adobe vydala bezpečnostné aktualizácie svojich produktov, ktoré opravujú 165 zraniteľností, z čoho 45 sú označené ako kritické. Kritické zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vykonanie škodlivého kódu, eskaláciu privilégií a získanie neoprávneného prístupu k citlivým údajom. Ostatné zraniteľnosti umožňujú vykonanie škodlivého kódu, získanie neoprávneného prístupu k citlivým údajom, obídenie bezpečnostných prvkov a zneprístupnenie služby. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ ZRANITEĽNOSŤ V NÁSTROJOCH PRE ZABEZPEČENÝ PRENOS SÚBOROV OD SPOLOČNOSTI CLEO

Bezpečnostní výskumníci zo spoločnosti Huntress informovali o aktívne zneužívanej zraniteľnosti v nástrojoch pre zabezpečený prenos a zdieľanie súborov Cleo Harmony, Cleo VLTrader a Cleo LexiCom. Zraniteľnosť CVE-2024-55956 možno zneužiť na získanie neoprávneného prístupu k citlivým údajom, vykonanie neoprávnených zmien v systéme a vzdialené vykonanie kódu. Zraniteľnosť v súčasnosti zneužíva aj ransomvérová skupina Clop. Viac informácií na stránke.

KRITICKÉ BEZPEČNOSTNÉ ZRANITEĽNOSTI V PRODUKTOCH IVANTI CSA, ICS A IPS

Spoločnosť Ivanti vydala bezpečnostné aktualizácie, ktoré opravujú 8 bezpečnostných zraniteľností v produktoch Ivanti Cloud Services Application (CSA), Ivanti Desktop and Server Management (DSM), Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS), Sentry a Patch SDK, z čoho 5 je označených ako kritické. Kritické zraniteľnosti v produktoch CSA, ICS a IPS možno zneužiť na SQL injekciu, vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

ZRANITEĽNOSTI SSL-VPN V ZARIADENIACH SÉRIE SMA100 OD SPOLOČNOSTI SONICWALL

Spoločnosť SonicWall vydala bezpečnostné aktualizácie, ktoré opravujú 6 zraniteľností vo funkcionalite SSL-VPN zariadení série SMA100. Najzávažnejšie zraniteľnosti s označením CVE-2024-53703, CVE-2024-45318, CVE-2024-40763 a CVE-2024-38475 možno zneužiť na vzdialené vykonanie kódu a získanie neoprávneného prístupu k citlivým údajom. Viac informácií na stránke.

VYSOKO ZÁVAŽNÁ ZRANITEĽNOSŤ V PLUGINE WORDPRESS WPFORMS

Vývojári WordPress pluginu WPForms vydali bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť. CVE-2024-11205 možno vykonaním neoprávnených zmien v systéme zneužiť vrátenie platieb alebo zrušenie predplatného implementovaného prostredníctvom služby Stripe a spôsobiť tak finančné škody prevádzkovateľom zraniteľných webových stránok. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ MANAŽMENTOVÉHO NÁSTROJA VEEAM SERVICE PROVIDER CONSOLE

Spoločnosť Veeam vydala bezpečnostné aktualizácie nástroja Veeam Service Provider Console (VSPC), ktoré opravujú dve zraniteľnosti, z čoho jedna je označená ako kritická. CVE-2024-42448 možno zneužiť na vzdialené vykonanie kódu na serveroch VSPC. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V IAM SYSTÉME SAILPOINT IDENTITYIQ

Spoločnosť SailPoint vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť v produkte IdentityIQ. Jedná sa o IAM (Identity and Access Management) platformu pre overovanie identity používateľov. CVE-2024-10905 možno zneužiť na získanie neoprávneného prístupu k citlivým údajom a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

BEZPEČNOSTNÍ VÝSKUMNÍCI ZVEREJNILI POC KÓD PRE ZNEUŽITIE KRITICKEJ ZRANITEĽNOSTI V PROGRESS WHATSUP GOLD

Bezpečnostní výskumníci zo spoločnosti Tenable zverejnili proof-of-concept kód demonštrujúci postup zneužitia kritickej zraniteľnosti v produkte Progress WhatsUp Gold, ktorá bola opravená aktualizáciami zo septembra 2024. CVE-2024-8785 možno zneužiť na vykonanie neoprávnených zmien v systéme a následné vykonanie škodlivého kódu. Viac informácií na stránke.