MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

NOVEMBER 2024

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci november 2 kritické a 35 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritickú zraniteľnosť **CVE-2024-43625** v komponente **Windows VMSwitch**, ktorý je súčasťou hypervízora Hyper-V, možno zneužiť na **eskaláciu privilégií** na úroveň oprávnení SYSTEM a následné vykonanie škodlivého kódu. Lokálny útočník by predmetnú zraniteľnosť mohol zneužiť zaslaním špeciálne vytvorenej sekvencie sieťových požiadaviek na ovládač VMSwitch, ktoré by umožnili použitie odalokovaného miesta v pamäti na Hyper-V hoste.

CVE-2024-43639 (CVSS skóre 9,8) spočíva v chybnom skracovaní čísel pri konverzii dátových typov v kryptografickom protokole použitom v rámci komponentu **Windows Kerberos**. Vzdialený neautentifikovaný útočník by ju prostredníctvom špeciálne vytvorenej aplikácie mohol zneužiť na **vzdialené vykonanie kódu**.

Komponent **Windows SMBv3 Server** obsahuje zraniteľnosť s označením **CVE-2024-43447**, ktorá spočíva v dvojitom uvoľnení miesta v pamäti. Vzdialený neautentifikovaný útočník by ju mohol zneužiť na vzdialené vykonanie škodlivého kódu. Zraniteľnosť je možné zneužiť len v prípade použitia SMB over QUIC.

Vysoko závažné zraniteľnosti v komponente **Windows Telephony Service (CVE-2024-43620, CVE-2024-43621, CVE-2024-43622, CVE-2024-43627, CVE-2024-43628, CVE-2024-43635)** by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému. Zraniteľnosti spočívajú v podtečení celočíselnej premennej a pretečení medzipamäte haldy. Zneužitie zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí iniciovať spojenie na server pod kontrolou útočníka.

Zraniteľnosť v rámci **Active Directory Certificate Services (CVE-2024-49019)** umožňuje lokálnemu autentifikovanému útočníkovi zneužiť zabudované vzory certifikátov (napr. WebServer template) na vytvorenie CSR (Certificate Signing Request) požiadaviek vedúcich k eskalácii privilégií na úroveň doménového administrátora. Zraniteľné sú všetky certifikáty vytvorené použitím templatu verzie 1, na ktorých je pole „Source of subject name“ nastavené na hodnotu „Supplied in the request“ a vzory nie sú zabezpečené podľa návodu pre zabezpečenie PKI od

spoločnosti Microsoft. Zraniteľnosť objavili bezpečnostní výskumníci zo spoločnosti TrustedSec, ktorá zverejnila aj kompletnú analýzu.

Ostatné zraniteľnosti vysokej závažnosti možno zneužiť na eskaláciu privilégií, zneprístupnenie služby, obídenie bezpečnostných prvkov, realizáciu spoofing útokov alebo získanie neoprávneného prístupu k citlivým údajom.

ZRANITEĽNÉ SYSTÉMY:

- 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 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-2024-43625
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43639

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

Kritická zraniteľnosť v produkte **Microsoft Copilot Studio (CVE-2024-49038)** spočíva v nedostatočnom overovaní vstupov pri generovaní webových stránok a vzdialený neautentifikovaný útočník by ju mohol zneužiť na získanie neoprávneného prístupu do systému a **eskaláciu privilégií**. Zraniteľnosť bola automaticky opravená spoločnosťou Microsoft a nevyžaduje dodatočnú aktualizáciu systémov.

Microsoft Excel obsahuje zraniteľnosti spočívajúce v nesprávnom overovaní špeciálnych elementov v rámci príkazov (**CVE-2024-49026**), použití odalokovaného miesta v pamäti (**CVE-2024-49027**), čítaní mimo povolených hodnôt (**CVE-2024-49028**), využití neinicializovaných zdrojov (**CVE-2024-49029**) a pretečení medzipamäte haldy (**CVE-2024-49030**). Vzdialený neautentifikovaný útočník by ich podvrhnutím špeciálne vytvorených súborov mohol zneužiť na **vzdialené vykonanie škodlivého kódu**. Zneužitie zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí stiahnuť a otvoriť škodlivé súbory.

CVE-2024-49031 a **CVE-2024-49032** sa nachádzajú v komponente **Microsoft Office Graphics** a vzdialený neautentifikovaný útočník by ich mohol zneužiť na vzdialené vykonanie kódu. Zneužitie zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí stiahnuť a otvoriť špeciálne vytvorené súbory.

Zraniteľnosť s označením **CVE-2024-49033** v produkte **Microsoft Word** spočíva v nedostatočnom overovaní vstupov a možno ju zneužiť na **obídenie bezpečnostného mechanizmu Office Protected View**. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť špeciálne vytvorený súbor.

Zraniteľnosť v **Microsoft PC Manager** spočíva v nesprávnom preklade odkazov pri otváraní súborov a vzdialený autentifikovaný útočník by ju mohol zneužiť na **eskaláciu privilégií** a vykonanie neoprávnených zmien v systéme (odstránenie systémových súborov). Zraniteľnosti bol pridelený identifikátor **CVE-2024-49051** a je ju možné zneužiť spustením špeciálne vytvorenej aplikácie.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft 365 Apps for Enterprise for 64-bit Systems

- Microsoft Copilot Studio
- Microsoft Excel 2016 (32-bit edition)
- Microsoft Excel 2016 (64-bit edition)
- Microsoft Excel 2016 Click-to-Run (C2R) for 32-bit editions
- Microsoft Excel 2016 Click-to-Run (C2R) for 64-bit editions
- 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 Office Online Server
- Microsoft PC Manager
- 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-2024-49038
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49026
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49027
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49028

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49029
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49030
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49031
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49032
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49033
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49051

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 október 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 november opravila 1 vysoko závažnú zraniteľnosť vo webovom prehliadači Microsoft Edge.

Zraniteľnosť s označením CVE-2024-49054 možno zneužiť v rámci spoofing útokov. Zneužitie zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí kliknúť na špeciálne vytvorený URL odkaz. V prípade veľmi dlhých URL odkazov v prehliadači dochádza k orezaniu časti názvu navštívenej domény.

ZRANITEĽNÉ SYSTÉMY:

- Microsoft Edge verzie staršie ako 131.0.2903.63
- Microsoft Edge (Chromium-based) verzie staršej ako 131.0.6778.85/.86

ODPORÚČANIA:

Odporúčame aktualizovať Microsoft Edge aspoň na verziu 131.0.2903.63 a Chromium-based na verziu 131.0.6778.85/.86.

ZDROJE:

- https://msrc.microsoft.com/update-guide/en-us
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49054

MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci november opravila 2 vysoko závažné zraniteľnosti v línii internetových prehliadačov Firefox a Firefox ESR.

Bližšie nešpecifikovanú zraniteľnosť s označením **CVE-2024-11699** (línie Firefox, Firefox ESR) možno zneužiť na **poškodenie obsahu pamäte** a **vzdialené vykonanie škodlivého kódu**. Obe línie prehliadačov obsahujú zraniteľnosť **CVE-2024-11691** súvisiacu s chybou v grafických ovládačoch zariadení Apple Silicon M Series, ktorú bližšie nešpecifikovanými WebGL operáciami možno zneužiť na zápis mimo povolených hodnôt a následné **poškodenie obsahu pamäte**. Pozn.: Zraniteľnosť je možné zneužiť len na zariadeniach Apple M Series.

Zneužitie oboch zraniteľností **vyžaduje interakciu zo strany používateľa**, ktorý musí otvoriť špeciálne vytvorený webový obsah.

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox verzie staršie ako 133
- Mozilla Firefox ESR verzie staršej ako 128.5

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 133 a Firefox ESR na verziu 128.5.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-65/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-64/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-63/
- https://nvd.nist.gov/vuln/detail/CVE-2024-11691
- https://nvd.nist.gov/vuln/detail/CVE-2024-11699

GOOGLE CHROME

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

Zraniteľnosti v komponentoch Family Experiences (CVE-2024-10826) a Serial (CVE-2024-10827) spočívajú v použití odalokovaného miesta v pamäti a možno ich zneužiť na **vzdialené vykonanie kódu**. Nesprávne vyhodnocovanie dátových typov v rámci komponentu V8 (CVE-2024-11395) možno zneužiť na **vzdialené vykonanie kódu**.

Posledná zraniteľnosť s identifikátorom CVE-2024-11110 sa nachádza v komponente Blink a vzdialený neautentifikovaný útočník by ju podvrhnutím špeciálne vytvoreného webového obsahu mohol zneužiť na **obídenie bezpečnostných mechanizmov prehliadača**.

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 131.0.6778.85/.86
- Google Chrome pre Linux verzie staršej ako 131.0.6778.85

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 131.0.6778.85/.86 a Linux verzie aspoň na verziu 131.0.6778.85.

ZDROJE:

- https://chromereleases.googleblog.com/2024
- https://chromereleases.googleblog.com/2024/11/stable-channel-update-for-desktop_19.html
- https://chromereleases.googleblog.com/2024/11/stable-channel-update-for-desktop_12.html
- https://chromereleases.googleblog.com/2024/11/stable-channel-update-for-desktop.html
- https://exchange.xforce.ibmcloud.com/vulnerabilities/387127
- https://exchange.xforce.ibmcloud.com/vulnerabilities/387126
- https://exchange.xforce.ibmcloud.com/vulnerabilities/388227
- https://exchange.xforce.ibmcloud.com/vulnerabilities/389299

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 opravila 1 kritickú a 1 vysoko závažnú zraniteľnosť vo frameworku .NET.

Kritická zraniteľnosť CVE-2024-43498 vo frameworku .NET a produkte Visual Studio spočíva v nesprávnom vyhodnocovaní dátových typov a vzdialený neautentifikovaný útočník by ju mohol zneužiť na vzdialené vykonanie kódu. Zraniteľnosť možno zneužiť zaslaním špeciálne vytvorenej požiadavky na zraniteľnú webovú aplikáciu vytvorenú v .NET alebo nahraním špeciálne vytvoreného súboru do desktopovej aplikácie Visual Studio.

Vysoko závažná zraniteľnosť CVE-2024-43499 spočíva v nesprávnom spracovaní dát s vysokou úrovňou kompresie a možno ju zneužiť na zneprístupnenie služby.

ZRANITEĽNÉ SYSTÉMY:

- .NET 9.0 inštalované na zariadeniach s operačným systémom Linux
- .NET 9.0 inštalované na zariadeniach s operačným systémom Mac OS
- .NET 9.0 inštalované na zariadeniach s operačným systémom Windows
- Microsoft Visual Studio 2022 version 17.11
- Microsoft Visual Studio 2022 version 17.10
- Microsoft Visual Studio 2022 version 17.6
- Microsoft Visual Studio 2022 version 17.8

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-2024-43498
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43499

ORACLE JAVA

Spoločnosť Oracle plánuje vydať veľkú sadu opráv 21. januára 2025.

ZDROJE:

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

6. INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

ZRANITEĽNOSŤ WORDPRESS PLUGINU LITESPEED CACHE UMOŽŇUJE ZÍSKANIE ADMINISTRÁTORSKÉHO PRÍSTUPU

Vývojári populárneho pluginu WordPress LiteSpeed Cache vydali bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú bezpečnostnú zraniteľnosť. CVE-2024-50550 možno zneužiť na eskaláciu privilégií a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ QNAP QUROUTER

Spoločnosť QNAP vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zero-day zraniteľnosť vo svojom operačnom systéme QuRouter. Bližšie nešpecifikovanú zraniteľnosť s označením CVE-2024-50389 možno zneužiť na získanie úplnej kontroly nad zariadením. Informácie o druhu zraniteľnosti neboli zverejnené. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V PRODUKTE CISCO UNIFIED INDUSTRIAL WIRELESS SOFTWARE

Spoločnosť Cisco vydala bezpečnostné aktualizácie svojho produktu Cisco Unified Industrial Wireless Software, ktoré opravujú kritickú zraniteľnosť. Produkt je využívaný v rámci URWB (Ultra Reliable Wireless Backhaul) prístupových bodov určených pre priemyselné siete. CVE-2024-20418 možno zneužiť na vzdialené vykonanie príkazov. Viac informácií na stránke.

ZRANITEĽNOSŤ V SQLITE OBJAVIL MODEL AI OD GOOGLE

Tím Google Project Zero testoval využitie modelu umelej inteligencie Big Sleep pri hľadaní zraniteľností v známych open source produktoch. Model úspešne objavil zraniteľnosť v SQLite, ktorú neodhalili fuzzingové nástroje. Zraniteľnosť súvisí s podtečením medzipamäte zásobníka, čo môže viesť k schopnosti zapisovať na halde mimo povolené hodnoty. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V PRÍSTUPOVÝCH BODOCH OD HPE ARUBA NETWORKING

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostné aktualizácie, ktoré opravujú 6 zraniteľností v operačných systémoch Instant AOS-8 a AOS-10 používaných v prístupových bodoch Aruba Series, z čoho 2 sú označené ako kritické. Zraniteľnosti CVE-2024-42509 a CVE-

2024-47460 možno zneužiť na injekciu príkazov a vzdialené vykonanie škodlivého kódu. Viac informácií na stránke.

ZRANITEĽNOSŤ VO VEEAM BACKUP ENTERPRISE MANAGER MOŽNO ZNEUŽIŤ NA OBÍDENIE MECHANIZMOV AUTENTIFIKÁCIE

Spoločnosť Veeam vydala bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť v produkte Veeam Backup Enterprise Manager (VBEM). Zraniteľnosť CVE-2024-40715 možno zneužiť na obídenie mechanizmov autentifikácie. Viac informácií na stránke.

KRITICKÉ BEZPEČNOSTNÉ ZRANITEĽNOSTI V PRODUKTOCH IVANTI EPM, ICS A IPS

Spoločnosť Ivanti vydala bezpečnostné aktualizácie, ktoré opravujú 43 bezpečnostných zraniteľností v produktoch Ivanti Endpoint Manager (EPM), Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS) a Ivanti Secure Access Client (ISAC), z čoho 9 je označených ako kritických. Kritické zraniteľnosti možno zneužiť na vzdialené vykonanie kódu. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V ROUTROCH D-LINK DSL6740C S UKONČENOU TECHNICKOU PODPOROU

Bezpečnostní výskumníci zverejnili informácie o 7 zraniteľnostiach routrov D-LINK DSL6740C, z ktorých jedna je označená ako kritická. Kritickú zraniteľnosť CVE-2024-11068 možno zneužiť na získanie úplnej kontroly na zariadením. Ostatné zraniteľnosti možno zneužiť na injekciu príkazov a získanie neoprávneného prístupu k citlivým údajom. Viac informácií na stránke.

BEZPEČNOSTNÉ ZRANITEĽNOSTI V PRODUKTOCH ADOBE

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty Adobe Bridge, Audition, After Effects, Substance 3D Painter, Illustrator, InDesign, Photoshop a Commerce, ktoré opravujú 48 zraniteľností, z čoho 28 sú označené ako kritické. Najzávažnejšie zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vykonanie škodlivého kódu. Viac informácií na stránke.

MICROSOFT V RÁMCI NOVEMBROVÉHO PATCH TUESDAY OPRAVIL 4 KRITICKÉ ZRANITEĽNOSTI

Spoločnosť Microsoft vydala v novembri 2024 balík opráv pre portfólio svojich produktov opravujúci 89 zraniteľností, z ktorých 52 umožňuje vzdialené vykonávanie kódu. Kritické zraniteľnosti sa nachádzajú vo frameworku .NET, produkte Visual Studio, komponentoch

Windows VMSwitch a Window Kerberos a online platforme airlift.microsoft.com a možno ich zneužiť na eskaláciu privilégií a vzdialené vykonanie škodlivého kódu. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ KRITICKÁ ZRANITEĽNOSŤ PALO ALTO PAN-OS

Spoločnosť Palo Alto Networks vydala varovanie ohľadom bližšie nešpecifikovanej kritickej zraniteľnosti v manažmentovom rozhraní firewallov, ktorá umožňuje vzdialené vykonávanie príkazov. Zraniteľnosť je aktívne zneužívaná a existuje na ňu verejne dostupný exploit. Viac informácií na stránke.

ZÁVAŽNÁ ZRANITEĽNOSŤ POSTGRESQL UMOŽŇUJE VYKONÁVAŤ KÓD

V PostgreSQL bola opravená vysoko závažná zraniteľnosť súvisiaca s nevhodnou kontrolou premenných prostredia v PL/Perl. Jej zneužitím môže útočník získať schopnosť vykonávať ľubovoľný kód, získať citlivé informácie, alebo vykonať inú činnosť v závislosti napríklad od zneužitej premennej.. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ MODULU WORDPRESS REALLY SIMPLE SECURITY

Vývojári modulu WordPress Really Simple Security opravili kritickú zraniteľnosť, ktorá umožňuje neprihlásenému útočníkovi získať neoprávnený prístup do zraniteľného systému ako ľubovoľný používateľ, vrátane administrátora. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ KRITICKÁ ZRANITEĽNOSŤ ZARIADENÍ GEOVISION

Viacero produktov spoločnosti GeoVision s ukončenou podporou zneužívajú útočníci pre variant botnetu MIRAI. Infekcia prebieha po zneužití kritickej zraniteľnosti, ktorá umožňuje vykonávanie systémových príkazov bez potreby autentifikácie. Viac informácií na stránke.

ZRANITEĽNOSŤ KNIŽNICE QUERYDSL A OPENFEIGN QUERYDSL UMOŽŇUJÚCA SQL/HQL INJECTION

Bezpečnostní analytici CSIRT.SK objavili zraniteľnosť CVE-2024-49203 v Java knižnici Querydsl a OpenFeign Querydsl, ktorá umožňuje vykonávať útoky typu SQL/HQL injection. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÉ ZERO-DAY ZRANITEĽNOSTI V OPERAČNÝCH SYSTÉMOCH MACOS, IOS, IPADOS A VISIONOS A PREHLIADAČI SAFARI

Spoločnosť Apple vydala bezpečnostné aktualizácie, ktoré opravujú 2 aktívne zneužívané zero-day zraniteľnosti v komponentoch operačných systémov macOS, iOS, iPadOS a visionOS a

internetovom prehliadači Safari. CVE-2024-44308 by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu a CVE-2024-44309 na realizáciu XSS útokov. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V ROUTROCH D-LINK S UKONČENOU TECHNICKOU PODPOROU

Spoločnosť D-Link varovala pred kritickou bezpečnostnou zraniteľnosťou v routroch DSR-150, DSR-150N, DSR-250, DSR-250N a DSR-1000N s ukončenou technickou podporou. Bližšie nešpecifikovaná kritická zraniteľnosť umožňuje vzdialené vykonanie kódu. Viac informácií na stránke.

ZRANITEĽNOSTI V LINUXOVOM NÁSTROJI NEEDRESTART UMOŽŇUJÚ ZÍSKANIE ÚPLNEJ KONTROLY NAD SYSTÉMOM

Vývojári linuxového nástroja needrestart vydali bezpečnostné aktualizácie, ktoré opravujú 5 zraniteľností. Zraniteľnosti s označením CVE-2024-48990, CVE-2024-48991, CVE-2024-48992, CVE-2024-10224 a CVE-2024-11003 by lokálny autentifikovaný útočník mohol zneužiť na získanie úplnej kontroly nad systémom. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ ZERO-DAY ZRANITEĽNOSŤ V ORACLE AGILE PLM FRAMEWORK

Spoločnosť Oracle vydala bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú zero-day zraniteľnosť v produkte Agile Product Lifecycle Management (PLM) Framework. CVE-2024-21287 možno zneužiť na získanie neoprávneného prístupu k citlivým údajom. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ VO FUNKCII JAZYKA PHP

Bezpečnostný výskumník Yiheng Cao objavil kritickú zraniteľnosť vyskytujúcu sa v implementácii PHP funkcie ldap_escape() na 32-bitových systémoch. Táto zraniteľnosť súvisí s pretečením medzipamäte, čo umožňuje zápis do pamäte mimo povolené hodnoty. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V KOMPRIMAČNOM NÁSTROJI 7-ZIP

Vývojári komprimačného nástroja 7-Zip vydali bezpečnostné aktualizácie, ktoré opravujú kritickú bezpečnostnú zraniteľnosť. CVE-2024-11477 možno podvrhnutím špeciálne vytvorených súborov zneužiť na vzdialené vykonanie kódu. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI BEZDRÔTOVÝCH PRÍSTUPOVÝCH BODOV ADVANTECH EKI

Spoločnosť Advantech vydala bezpečnostné aktualizácie na svoje priemyselné bezdrôtové prístupové body (access pointy) série EKI, ktoré opravujú 20 zraniteľností, z čoho 6 je označených ako kritické. CVE-2024-50370 až CVE-2024-50375 možno zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

AKTÍVNE ZNEUŽÍVANÁ ZRANITEĽNOSŤ V PLATFORME PROJECTSEND

Bezpečnostní výskumníci zo spoločnosti VulnCheck varovali pred aktívnym zneužívaním kritickej zraniteľnosti v open source platforme pre zdieľanie súborov ProjectSend. CVE-2024-11680 možno zneužiť na vykonanie škodlivého kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V PRODUKTOCH QNAP

Spoločnosť QNAP vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú 8 zraniteľností, z čoho 3 sú označené ako kritické. Kritické zraniteľnosti v produkte Notes Station 3 (CVE-2024-38643, CVE-2024-38645) a routeroch QuRouter (CVE-2024-48860) možno zneužiť na realizáciu SSRF útokov, získanie neoprávneného prístupu k citlivým údajom a získanie úplnej kontroly nad systémom. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI VO WORDPRESS PLUGINE SPAM PROTECTION, ANTI-SPAM, FIREWALL

Vývojári WordPress pluginu Spam Protection, Anti-Spam, FireWall vydali bezpečnostné aktualizácie, ktoré opravujú 2 kritické zraniteľnosti. Zraniteľnosti s označením CVE-2024-10542 a CVE-2024-10781 možno zneužiť na inštaláciu, odstránenie, aktiváciu a deaktiváciu ľubovoľných pluginov redakčného systému a následné získanie úplnej kontroly nad systémom. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V MONITOROVACEJ PLATFORME ZABBIX

Vývojári monitorovacej platformy Zabbix vydali bezpečnostné aktualizácie, ktoré opravujú 4 zraniteľnosti, z čoho 2 sú označené ako kritické. Kritické zraniteľnosti s identifikátormi CVE-2024-42330 a CVE-2024-42327 možno zneužiť na eskaláciu privilégií, vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Viac informácií na stránke.