MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

SEPTEMBER 2024

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci september 2 kritické a 43 vysoko závažných zraniteľností v operačných systémoch Windows.

Komponent Windows Network Address Translation obsahuje kritickú zraniteľnosť s označením CVE-2024-38119, ktorá spočíva v použití odalokovaného miesta v pamäti a možno ju zneužiť na vykonanie škodlivého kódu. Zneužitie zraniteľnosti vyžaduje, aby sa útočník nachádzal v rovnakom sieťovom segmente.

Kritická zraniteľnosť v komponente Windows Update spočíva v použití odalokovaného miesta v pamäti a vzdialený neautentifikovaný útočník by ju prostredníctvom zaslania špeciálne vytvorenej požiadavky mohol zneužiť na vykonanie škodlivého kódu. CVE-2024-43491 je v súčasnosti aktívne zneužívaná útočníkmi.

CVE-2024-43495 v komponente Windows libarchive spočíva v pretečení celočíselnej premennej a vzdialený autentifikovaný útočník s oprávneniami úrovne „guest“ by ju mohol zneužiť na vzdialené vykonanie kódu. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť škodlivý súbor RAR zaslaný útočníkom.

Zraniteľnosť CVE-2024-38259 v komponente Microsoft Management Console spočíva v použití odalokovaného miesta v pamäti a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvoreného súboru mohol zneužiť na vzdialené vykonanie škodlivého kódu. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa, ktorý musí stiahnuť a spustiť škodlivý súbor.

Vysoko závažné zraniteľnosti v komponentoch Windows TCP/IP (CVE-2024-21416, CVE-2024-38045), Windows Remote Desktop Licensing Service (CVE-2024-38260, CVE-2024-38263, CVE-2024-43454, CVE-2024-43467) umožňujú vzdialené vykonanie kódu.

Ostatné zraniteľnosti vysokej závažnosti možno zneužiť na eskaláciu privilégií, zneprístupnenie služby, obídenie bezpečnostného prvku 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 11 version 21H2 for ARM64-based Systems
- Windows 11 version 21H2 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)

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-2024-38119
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43491

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 september bezpečnostné aktualizácie, ktoré opravujú 3 kritické a 10 vysoko závažných zraniteľnosti v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritické zraniteľnosti v produkte Microsoft SharePoint spočívajú v deserializácii nedôveryhodných dát a umožňujú vzdialené vykonanie škodlivého kódu. Pre úspešné zneužitie zraniteľnosti CVE-2024-38018 musí útočník disponovať oprávneniami úrovne „Site Member“ a vyššie. Zneužitie zraniteľnosti s označením CVE-2024-43464 vyžaduje oprávnenia úrovne „Site Owner“ a vyššie a možno ju zneužiť nahraním špeciálne vytvoreného súboru a následným zaslaním špeciálne vytvorenej API požiadavky, ktorá vedie k deserializácii parametrov tohto súboru.

Kritická zraniteľnosť CVE-2024-38183 v produkte GroupMe spočíva v nesprávnej implementácii mechanizmov riadenia prístupu. Vzdialený neautentifikovaný útočník by ju prostredníctvom SSRF útoku mohol zneužiť na eskaláciu privilégií. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť škodlivý URL odkaz. Zraniteľnosť bola automaticky opravená spoločnosťou Microsoft a nevyžaduje dodatočnú aktualizáciu systémov.

Ostatné zraniteľnosti vysokej závažnosti umožňujú vzdialené vykonanie kódu, eskaláciu privilégií, zneprístupnenie služby, obídenie bezpečnostného prvku a získanie neoprávneného prístupu k citlivým údajom.

ZRANITEĽNÉ SYSTÉMY:

- GroupMe
- 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 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 for Mac 2021
- Microsoft Office Online Server
- Microsoft Office for Android
- Microsoft Office for Universal
- Microsoft Publisher 2016 (32-bit edition)
- Microsoft Publisher 2016 (64-bit edition)
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription Edition
- Microsoft Visio 2016 (32-bit edition)
- Microsoft Visio 2016 (64-bit edition)
- Outlook for iOS

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-2024-38018
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38183
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43464

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 máj 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 september opravila 2 vysoko závažné zraniteľnosti vo webovom prehliadači Microsoft Edge.

Zraniteľnosti s označením CVE-2024-43489 a CVE-2024-43496 spočívajú v nesprávnej manipulácii s dátovými typmi a zápise mimo povolených hodnôt. Vzdialený neautentifikovaný útočník by ich mohol zneužiť na vzdialené vykonanie škodlivého kódu. Zneužitie zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí kliknúť na špeciálne vytvorený URL odkaz.

ZDROJE:

- https://msrc.microsoft.com/update-guide/en-us
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43489
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43496

MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci september opravila 4 vysoko závažné zraniteľnosti v línii internetových prehliadačov Firefox a Firefox ESR.

Zraniteľnosti CVE-2024-8387 (Firefox, Firefox ESR) a CVE-2024-8389 (línia Firefox) bezpečnostné chyby pamäte a vzdialený neautentifikovaný útočník by ich mohol zneužiť na vzdialené vykonanie škodlivého kódu alebo zneprístupnenie služby.

Ostatné zraniteľnosti prítomné v oboch líniách prehliadačov spočívajú v nesprávnej manipulácii s dátovými typmi pri vyhľadávaní názvov vlastností objektov (CVE-2024-8381) a rozdielnom spracovávaní StructFields a ArrayTypes v rámci WASM (CVE-2024-8385). Uvedené zraniteľnosti umožňujú vzdialené vykonanie kódu alebo zneprístupnenie služby.

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

ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox verzie staršie ako 130
- Mozilla Firefox ESR verzie staršej ako 128.2

ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 130 a Firefox ESR na verziu 128.2.

ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-41/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-40/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-39/
- https://exchange.xforce.ibmcloud.com/vulnerabilities/352472
- https://exchange.xforce.ibmcloud.com/vulnerabilities/352473
- https://exchange.xforce.ibmcloud.com/vulnerabilities/352471
- https://exchange.xforce.ibmcloud.com/vulnerabilities/352474

GOOGLE CHROME

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

Komponenty WebAudio (CVE-2024-8362), Media Router (CVE-2024-8637), Autofill (CVE-2024-8639) a Dawn (CVE-2024-9120) obsahujú zraniteľnosti spočívajúce v použití odalokovaného miesta v pamäti. Vzdialený neautentifikovaný útočník by ich mohol zneužiť na vykonanie škodlivého kódu.

Zápis mimo povolených hodnôt (CVE-2024-7970), nesprávne vyhodnocovanie dátových typov (CVE-2024-8638, CVE-2024-8904, CVE-2024-9122) v komponente V8 by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu mohol zneužiť na vykonanie škodlivého kódu. Zraniteľnosť s označením CVE-2024-9121 možno zneužiť na obídenie bezpečnostných prvkov prehliadača.

Komponent Skia obsahuje 2 bezpečnostné zraniteľnosti spočívajúce v pretečení medzipamäte haldy (CVE-2024-8636) a celočíselnej premennej (CVE-2024-9123), ktoré možno zneužiť na vzdialené vykonanie kódu alebo zneprístupnenie služby.

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 129.0.6668.70/.71
- Google Chrome pre Linux verzie staršej ako 129.0.6668.70

ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 129.0.6668.70/.71 a Linux verzie aspoň na verziu 129.0.6668.70.

ZDROJE:

- https://chromereleases.googleblog.com/2024
- https://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_24.html
- https://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_17.html
- https://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_10.html
- https://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop.html

- https://exchange.xforce.ibmcloud.com/vulnerabilities/352415
- https://exchange.xforce.ibmcloud.com/vulnerabilities/352414
- https://exchange.xforce.ibmcloud.com/vulnerabilities/358706
- https://exchange.xforce.ibmcloud.com/vulnerabilities/358708
- https://exchange.xforce.ibmcloud.com/vulnerabilities/358709
- https://exchange.xforce.ibmcloud.com/vulnerabilities/358707
- https://exchange.xforce.ibmcloud.com/vulnerabilities/359938
- https://exchange.xforce.ibmcloud.com/vulnerabilities/363227
- https://exchange.xforce.ibmcloud.com/vulnerabilities/363228
- https://exchange.xforce.ibmcloud.com/vulnerabilities/363226
- https://exchange.xforce.ibmcloud.com/vulnerabilities/363225

4. ADOBE ACROBAT A READER

V mesiaci september spoločnosť Adobe vydala bezpečnostné aktualizácie, ktoré opravili 2 kritické zraniteľnosti v produkte Adobe Acrobat a Reader.

Kritické zraniteľnosti s označením CVE-2024-41869, CVE-2024-45112 spočívajú v použití odalokovaného miesta v pamäti a nesprávnej manipulácii s dátovými typmi. Vzdialený neautentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vzdialené vykonanie škodlivého kódu alebo zneprístupnenie služby.

Zneužitie všetkých zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť škodlivý súbor.

ZDROJE:

- https://helpx.adobe.com/security/security-bulletin.html#acrobat
- https://helpx.adobe.com/security/products/acrobat/apsb24-70.html
- https://exchange.xforce.ibmcloud.com/vulnerabilities/359373
- https://exchange.xforce.ibmcloud.com/vulnerabilities/359374

5. Frameworky

Microsoft .NET Framework

V mesiaci september spoločnosť Microsoft neopravila žiadne kritické ani vysoko závažné zraniteľnosti vo frameworku .NET.

Zdroje:

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

Oracle Java

Veľká sada opráv je plánovaná na 15. októbra 2024.

Zdroje:

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

6. Iné závažné zraniteľnosti

Zraniteľnosti v tlačovom subsystéme pre Unix a Linux možno zneužiť na vzdialené vykonanie kódu

Implementácia internetového tlačového protokolu IPP pre unixové systémy CUPS obsahuje 4 zraniteľnosti, z ktorých jedna je označená ako kritická. Zreťazením zraniteľností by vzdialený neautentifikovaný útočník mohol získať kontrolu nad parametrami v súbore PPD a možnosť vzdialene vykonávať kód. Viac informácií na stránke.

KRITICKÁ A ZÁVAŽNÉ ZRANITEĽNOSTI OPENPLC

Kyberbezpečnostná jednotka Talos spoločnosti Cisco zverejnila podrobnosti o viacerých opravených zraniteľnostiach v programovateľnom logickom ovládači OpenPLC, ktoré možno zneužiť pri útokoch DoS a na vzdialené vykonávanie kódu. Viac informácií na stránke.

ÚTOČNÍCI ZNEUŽÍVAJÚ KRITICKÚ ZRANITEĽNOSŤ IVANTI CLOUD SERVICES APPLIANCE

Spoločnosť Ivanti informovala o novej kritickej zraniteľnosti v produkte CSA, ktorá umožňuje získať prístup ku chráneným funkcionalitám. Útočníci ju zneužívajú v kombinácii s nedávno publikovanou zraniteľnosťou umožňujúcou vzdialené vykonávanie kódu. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ GITLAB

Spoločnosť GitLab vydala aktualizáciu opravujúcu kritickú zraniteľnosť, ktorá zasahuje autentifikačný proces na báze štandardu SAML. Chyba umožňuje neoverenému útočníkovi obísť prihlásenie. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ VO VMWARE VCENTER SERVER

Spoločnosť BROADCOM vydala bezpečnostné aktualizácie, opravujúce bezpečnostné chyby ovplyvňujúce VMware vCenter Server. Z nich 1 je označená ako kritická a 1 vysoko závažná. Zraniteľnosti možno zneužiť na eskaláciu privilégií a vzdialené vykonanie kódu. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI ROUTEROV D-LINK

Spoločnosť D-Link opravila tri kritické a dve vysoko závažné zraniteľnosti vo firmvéroch zariadení COVR-X1870, DIR-X4860 a DIR-X5460. Zraniteľnosti súvisia s napevno kódovanými prihlasovacími údajmi a ďalšími chybami, ktoré umožňujú vzdialene vykonávať kód, pristupovať k zariadeniam cez Telnet a vykonávať systémové príkazy. Viac informácií na stránke.

VYSOKO ZÁVAŽNÉ ZRANITEĽNOSTI V CISCO IOS XR

Spoločnosť CISCO vydala bezpečnostné aktualizácie na svoj operačný systém IOS XR, ktoré opravujú 8 zraniteľností, z čoho 6 je označených ako vysoko závažné. Zraniteľnosti s označením CVE-2024-20398, CVE-2024-20304, CVE-2024-20483, CVE-2024-20489, CVE-2024-20317 a CVE-2024-20406 možno zneužiť na injekciu príkazov, vykonanie škodlivého kódu, eskaláciu

privilégií, zneprístupnenie služby a získanie neoprávneného prístupu k citlivým údajom. Viac informácií na stránke.

GitLab opravuje kritickú a vysoko závažné zraniteľnosti

Spoločnosť GitLab vydala opravný balík pre 18 zraniteľností. Z toho jedna je hodnotená ako kritická a tri ako vysoko závažné. Chyby umožňujú vzdialene vykonávať príkazy, spôsobiť nedostupnosť služby alebo vykonať útoky typu SSRF (Server-side request forgery). Viac informácií na stránke.

Microsoft v rámci septembrového Patch Tuesday opravil 7 kritických zraniteľností

Spoločnosť Microsoft vydala v septembri 2024 balík opráv pre portfólio svojich produktov opravujúci 79 zraniteľností, z ktorých 19 umožňuje vzdialené vykonávanie kódu. Kritické zraniteľnosti sa nachádzajú v produktoch Microsoft SharePoint Server, Azure Web Apps a Azure Stack Hub a v komponentoch Windows Network Address Translation a Microsoft Windows Update a možno ich zneužiť na eskaláciu privilégií a vzdialené vykonanie škodlivého kódu. Zraniteľnosti s označením CVE-2024-38014, CVE-2024-38217, CVE-2024-38226, CVE-2024-43491 v Microsoft Publisher a komponentoch Windows Installer, MOTW (Mark of the Web) a Windows Update sú aktívne zneužívané útočníkmi. Viac informácií na stránke.

Bezpečnostné zraniteľnosti v produktoch Adobe

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty Media Encoder, Audition, After Effects, Premiere Pro, Illustrator, Acrobat Reader, ColdFusion a Photoshop, ktoré opravujú 29 zraniteľností, z čoho 19 sú označené ako kritické. Najzávažnejšie zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vzdialené vykonanie škodlivého kódu. Ostatné zraniteľnosti možno zneužiť na získanie neoprávneného prístupu k citlivým údajom, vykonanie neoprávnených zmien v systéme a zneprístupnenie služby. Viac informácií na stránke.

Bezpečnostné zraniteľnosti v produkte Ivanti Endpoint Management

Spoločnosť Ivanti vydala bezpečnostné aktualizácie, ktoré opravujú 16 bezpečnostných zraniteľností v produkte Endpoint Manager, z čoho 10 je označených ako kritických. Kritické zraniteľnosti možno zneužiť na vykonanie škodlivého kódu a získanie úplnej kontroly nad systémom. Ostatné zraniteľnosti možno zneužiť na eskaláciu privilégií, získanie neoprávneného prístupu k citlivým údajom a vykonanie neoprávnených zmien v systéme. Viac informácií na stránke.

KRITICKÉ ZRANITEĽNOSTI V PRODUKTOCH VEEAM

Spoločnosť Veeam opravila kritické zraniteľnosti v produktoch Backup & Replication (VBR), ONE, Service Provider Console a ďalších. Najzávažnejšia z nich umožňuje neautentifikovanému útočníkovi vzdialene vykonávať kód vo VBR. V balíku opráv spoločnosť vyriešila aj viacero ďalších vysoko závažných zraniteľností. Viac informácií na stránke.

CISCO OPRAVUJE DVE KRITICKÉ ZRANITEĽNOSTI V SMART LICENSING UTILITY

Aplikácia Cisco Smart Licensing Utility obsahuje dve kritické zraniteľnosti, ktoré umožňujú útočníkom získať prihlasovacie údaje pre prístup k API rozhraniu s administrátorskými oprávneniami. Viac informácií na stránke.

KRITICKÁ ZRANITEĽNOSŤ V APACHE OPEN FOR BUSINESS

V aplikácii Apache Open For Business bola opravená kritická zraniteľnosť umožňujúca vzdialené vykonávanie kódu bez potreby autentifikácie. Súvisí s nedostatočným overením oprávnení používateľa, ktorý sa pokúša priamo pristúpiť ku chráneným zdrojom. Viac informácií na stránke.