Mesačný prehľad kritických zraniteľností
Apríl 2024

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci apríl 91 vysoko závažných zraniteľností.

Vysoko závažné zraniteľnosti s označením CVE-2024-20678, CVE-2024-26179, CVE-2024-26195, CVE-2024-26200, CVE-2024-26202, CVE-2024-26205, CVE-2024-26208, CVE-2024-26210, CVE-2024-26214, CVE-2024-26221, CVE-2024-26222, CVE-2024-26223, CVE-2024-26224, CVE-2024-26227, CVE-2024-26231, CVE-2024-26232, CVE-2024-26233, CVE-2024-26244, CVE-2024-26252, CVE-2024-26253, CVE-2024-26256, CVE-2024-29050 a CVE-2024-29066 sa nachádzajú v komponentoch Compressed Folders (zip), Cryptographic Services, DHCP Server Service, DNS Server, Distributed File System (DFS), Message Queuing (MSMQ), Remote Procedure Call Runtime, Routing and Remote Access Service (RRAS), WDAC OLE DB Provider for SQL Server, WDAC SQL Server ODBC Driver, rndismp6.sys a možno ich zneužiť na vzdialené vykonanie škodlivého kódu.

Ostatné zraniteľnosti vysokej závažnosti umožňujú eskaláciu privilégií, zneprístupnenie služby, obchádzanie bezpečnostných prvkov 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 ARM64-based 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 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

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 apríl bezpečnostné aktualizácie, ktoré opravujú 2 vysoko závažné zraniteľnosti.

Zraniteľnosť v produkte Microsoft Sharepoint Server (CVE-2024-26251) spočíva v nedostatočnom overovaní vstupov počas generovania webových stránok a vzdialený útočník by ju mohol zneužiť na vykonanie XSS (Cross Site Scripting) útokov.

CVE-2024-26257 (Microsoft Excel) sa týka dvojitého uvoľnenia miesta pamäte a umožňuje vzdialené vykonanie škodlivého kódu.

Zneužitie oboch zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí kliknúť na špeciálne vytvorenú URL adresu alebo 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 Office LTSC for Mac 2021
Microsoft SharePoint Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription 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-2024-26251
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26257

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 apríl 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 apríl neopravila v prehliadači Microsoft Edge žiadnu kritickú ani závažnú zraniteľnosť.

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

Mozilla Firefox

Spoločnosť Mozilla v mesiaci apríl opravila 9 vysoko závažných zraniteľností v línii internetových prehliadačov Firefox a Firefox ESR.

CVE-2024-3853 (Firefox), CVE-2024-3856 (Firefox) a CVE-2024-3857 (Firefox, Firefox ESR) spočívajú v použití odalokovaného miesta v pamäti a možno ich zneužiť na zneprístupnenie služby alebo vykonanie škodlivého kódu.

Zraniteľnosti kompliátora JIT CVE-2024-3854 (línie Firefox aj Firefox ESR) a CVE-2024-3855 (len Firefox) môžu viesť k nesprávnej optimalizácii switch a MSubstr operácií a vygenerovať kód umožňujúci čítanie mimo povolených hodnôt.

Zraniteľnosti CVE-2024-3865 (Firefox, Firefox ESR) a CVE-2024-3864 (Firefox) možno zneužiť na poškodenie pamäte a následné vykonanie škodlivého kódu.

Nesprávnu dereferenciu ukazovateľov v rámci js::CheckTracedThing<js::Shape> (CVE-2024-3858) by vzdialený neautentifikovaný útočník mohol zneužiť na mutáciu objektov JavaScript vedúcu k zneprístupneniu služby.

Zraniteľnosť CVE-2024-3852 (Firefox, Firefox ESR) spočíva v nesprávnej optimalizácii funkcie GetBoundName počas JIT kompilácie a umožňuje obídenie bezpečnostných obmedzení.

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

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako Firefox 125
Mozilla Firefox ESR verzie staršej ako 115.10

Odporúčania:

Odporúčame aktualizovať Firefox na verziu 125 a Firefox ESR na verziu 115.10.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-18/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-19/

Google Chrome

V mesiaci apríl spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili celkom 1 kritickú a 14 vysoko závažných zraniteľností.

Kritická zraniteľnosť s označením CVE-2024-4058 spočíva v nesprávnom vyhodnotení typu premennej v rámci komponentu ANGLE a umožňuje vzdialené vykonanie kódu.

Vysoko závažné zraniteľnosti v komponentoch Picture in Picture (CVE-2024-4331), Dawn (CVE-2024-4368, CVE-2024-4060, CVE-2024-3515), V8 (CVE-2024-3914), Bookmarks (CVE-2024-3158) a Downloads (CVE-2024-3834) umožňujú zneužiť odalokované miesto v pamäti na vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

CVE-2024-4059, CVE-2024-3157 a CVE-2024-3159 v komponentoch V8 a Compositing umožňujú čítanie a zápis mimo povolených hodnôt a možno ich zneužiť na získanie neoprávneného prístupu k citlivým údajom alebo vykonanie škodlivého kódu.

Ostatné zraniteľnosti v komponentoch V8 (CVE-2024-3832, CVE-2024-3156), Web Assembly (CVE-2024-3833) a ANGLE (CVE-2024-3516) možno zneužiť na obídenie bezpečnostných mechanizmov, zneprístupnenie služby alebo vykonanie kódu.

Zraniteľné systémy:
Google Chrome pre Windows a Mac verzie staršej ako 124.0.6367.118/.119
Google Chrome pre Linux verzie staršej ako 124.0.6367.118

Odporúčania:
Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 124.0.6367.118/.119 a Linux verzie aspoň na verziu 124.0.6367.118.

Zdroje:
https://chromereleases.googleblog.com/2024/04
https://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_30.html
https://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_24.html
https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_16.html
https://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_10.html
https://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/289348
https://exchange.xforce.ibmcloud.com/vulnerabilities/289656
https://exchange.xforce.ibmcloud.com/vulnerabilities/289657
https://exchange.xforce.ibmcloud.com/vulnerabilities/289350
https://exchange.xforce.ibmcloud.com/vulnerabilities/287378
https://exchange.xforce.ibmcloud.com/vulnerabilities/288025
https://exchange.xforce.ibmcloud.com/vulnerabilities/286815
https://exchange.xforce.ibmcloud.com/vulnerabilities/287712
https://exchange.xforce.ibmcloud.com/vulnerabilities/289349
https://exchange.xforce.ibmcloud.com/vulnerabilities/287376
https://exchange.xforce.ibmcloud.com/vulnerabilities/286816
https://exchange.xforce.ibmcloud.com/vulnerabilities/287710
https://exchange.xforce.ibmcloud.com/vulnerabilities/286814
https://exchange.xforce.ibmcloud.com/vulnerabilities/287711
https://exchange.xforce.ibmcloud.com/vulnerabilities/287377

4. Adobe Acrobat a Reader

V produkte Adobe Acrobat a Reader neboli v mesiaci apríl opravené žiadne kritické ani vysoko závažné zraniteľnosti.

Zdroje:
https://helpx.adobe.com/security/security-bulletin.html#acrobat

5. Frameworky

Microsoft .NET Framework

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

Vysoko závažná zraniteľnosť s označením CVE-2024-21409 spočíva v použití odalokovaného miesta v pamäti a umožňuje vykonanie škodlivého kódu a získanie úplnej kontroly nad systémom. Zraniteľnosť možno zneužiť lokálne po prihlásení do zraniteľného systému alebo vzdialene prostredníctvom podvrhnutia škodlivých súborov, na ktoré musí obeť kliknúť.

Zraniteľné systémy:

.NET 6.0
.NET 7.0
.NET 8.0
Microsoft .NET Framework 3.5 AND 4.7.2
Microsoft .NET Framework 3.5 AND 4.8
Microsoft .NET Framework 3.5 AND 4.8.1
Microsoft .NET Framework 4.6.2
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 4.8

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 vyhľadávania.

Zdroje:

https://msrc.microsoft.com/update-guide/en-us
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21409

Oracle Java

Spoločnosť Oracle v mesiaci apríl vydala bezpečnostné aktualizácie, ktoré opravujú 2 vysoko závažné bezpečnostné zraniteľnosti v rámci Oracle Java SE.

Zraniteľnosť s označením CVE-2024-21892 sa nachádza v komponente Node.js v nesprávnej implementácii výnimky CAP_NET_BIND_SERVICE. Lokálny autentifikovaný útočník by ju mohol zneužiť na eskaláciu privilégií a následné narušenie dôvernosti a integrity systému.

Zraniteľnosť komponentu JavaFX (WebKitGTK) (CVE-2023-41993) by vzdialený útočník prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu mohol zneužiť na vykonanie škodlivého kódu. Zneužitie tejto zraniteľnosti vyžaduje interakciu zo strany používateľa.

Zraniteľné systémy:

Oracle GraalVM Enterprise Edition: 20.3.13, 21.3.9
Oracle GraalVM for JDK: 17.0.10, 21.0.2, 22
Oracle Java SE: 8u401

Odporúčania:

Odporúčame aktualizovať zraniteľné verzie Java SE na aktuálne verzie prostredníctvom Java Auto Update alebo na stránke spoločnosti Oracle, ktorú môžete nájsť v časti Zdroje.

Zdroje:
https://www.oracle.com/security-alerts/cpuapr2024.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/282986
https://exchange.xforce.ibmcloud.com/vulnerabilities/266672

6. Iné závažné zraniteľnosti

Ďalšie kritické zraniteľnosti v doplnkoch WordPress

Doplnky WP Automatic a WP Poll Maker obľúbenej platformy na tvorbu webových stránok obsahujú kritické zraniteľnosti, ktoré umožňujú bbchádzanie autentifikácie, vzdialené vykonávanie kódu, extrakcii citlivých údajov a získanie administrátorských oprávnení. Bolo zaznamenaných viac ako 5,5 milióna pokusov o aktívne zneužitie zraniteľností. **Viac informácií na stránke.**

Aktívne zneužívané zero-day zraniteľnosti Cisco

Spoločnosť Cisco poukázala na rozsiahlu kampaň pomenovanú ArcaneDoor, v ktorej útočníci zneužívajú dvoch zero-day zraniteľností CVE-2024-20353 a CVE-2024-20359. Úspešné zneužitie umožňuje útočníkom šíriť malvér a zbierať citlivé informácie v cieľovom prostredí. Cisco varovala, že sa jedná o aktívne zneužívané zraniteľnosti na firewalloch Cisco ASA a FTD hackerskou skupinou UAT4356 (alias Storm-1849). Spoločnosť zároveň opravila zraniteľnosť CVE-2024-20358, umožňujúcu injektovanie príkazov v spomínaných zariadeniach. **Viac informácií na stránke.**

Kritická zraniteľnosť v doplnku WordPress

Zásuvný modul Forminator obľúbenej platformy na tvorbu webových stránok obsahuje jednu kritickú a dve vysoko závažné zraniteľnosti. Chyby umožňujú nahrať a spustiť škodlivý kód na serveri stránky, únik citlivých informácií a odmietnutie služby. Zásuvný modul využíva viac ako 500 000 stránok. **Viac informácií na stránke.**

Aktívne zneužívaná zero-day zraniteľnosť v CrushFTP

Na aktívne zneužívanú bezpečnostnú chybu v produkte CrushFTP poukázal výskumník z Airbus CERT. Zero-day zraniteľnosť umožňuje neautentifikovanému útočníkovi uniknúť z virtuálneho súborového systému (VFS) a sťahovať systémové súbory. Tieto útoky sa údajne najviac

zameriavali na subjekty v USA, pričom existuje podozrenie, že mohli byť politicky motivované. **Viac informácií na stránke.**

Microsoft v rámci Patch Tuesday opravil aktívne zneužívané zraniteľnosti

Spoločnosť Microsoft opravila v rámci svojho pravidelného balíka aktualizácií Patch Tuesday 149 zraniteľností, z toho sú 3 kritické a 2 zero-day. Najzávažnejšie zraniteľnosti umožňujú eskaláciu oprávnení, vykonávanie kódu, únik informácií, či obchádzanie bezpečnostných prvkov. Zero-day zraniteľnosti CVE-2024-29988 a CVE-2024-26234 sú aktívne zneužívané. **Viac informácií na stránke.**

Kritická zraniteľnosť v softvéri Palo Alto PAN-OS

Spoločnosť Palo Alto Networks vydala bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú kritickú zraniteľnosti v softvéri PAN-OS. Verzie 10.2, 11.0 a 11.1 vo funkcii GlobalProtect obsahujú zraniteľnosť, ktorá umožňuje vzdialené vykonanie kódu. Zraniteľnosť je možné zneužiť len na firewalloch, na ktorých je zapnutá aspoň jedna z funkcií GlobalProtect Gateway alebo GlobalProtect Portal. **Viac informácií na stránke.**

Kritická zraniteľnosť v platforme Flowmon

Spoločnosť Progress vydala bezpečnostné aktualizácie platformy Flowmon pre meranie výkonnosti siete a bezpečnosti. Verzie staršie ako 11.1.14 a 12.3.5 obsahujú kritickú bezpečnostnú zraniteľnosť, ktorá umožňuje vzdialené vykonanie systémových príkazov. **Viac informácií na stránke.**

Bezpečnostné zraniteľnosti v produktoch Ivanti

Spoločnosť Ivanti vydala bezpečnostné aktualizácie, ktoré opravujú 4 bezpečnostné zraniteľnosti v produktoch Connect Secure a Policy Secure. Najzávažnejšie zraniteľnosti s označením CVE-2024-21894 a CVE-2024-22053 možno zneužiť na zneprístupnenie služby a vzdialené vykonanie škodlivého kódu. **Viac informácií na stránke.**

Kritická zraniteľnosť v doplnku WordPress

Doplnok obľúbenej platformy na tvorbu webových stránok obsahuje kritickú zraniteľnosť typu SQL injection, ktorá umožňuje neautentifikovaným útočníkom pripojiť ďalšie dotazy do existujúcich dotazov SQL. To môže viesť k neoprávnenému prístupu k citlivým informáciám

z databázy, ako napríklad hash hesiel. Chyba sa nachádza v zásuvnom module WordPress s názvom LayerSlider. **Viac informácií na stránke.**