Mesačný prehľad kritických zraniteľností
Jún 2024

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci jún 1 kritickú a 32 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritická zraniteľnosť v produkte Microsoft Message Queuing (MSMQ) spočíva vo využití odalokovaného miesta v pamäti a umožňuje vzdialenému neautentifikovanému útočníkovi vykonanie škodlivého kódu na MSMQ serveri. CVE-2024-30080 je možné zneužiť zaslaním sekvencie špeciálne vytvorených MSMQ paketov. Nakoľko sa jedná o voliteľnú súčasť operačných systémov Windows, zraniteľnosť možno zneužiť len na systémoch, kde je aktivovaná.

CVE-2024-30077 v komponente Windows OLE umožňuje vzdialené vykonanie škodlivého kódu a jej zneužitie vyžaduje, aby sa autentifikovaný používateľ pokúsil o pripojenie na škodlivú SQL databázu prostredníctvom ovládača OLE DB alebo OLEDB.

Pretečenie medzipamäte haldy v komponente Windows Routing and Remote Access Service (CVE-2024-30094, CVE-2024-30095) by útočník mohol zneužiť na vykonanie škodlivého kódu. Zneužitie zraniteľností vyžaduje interakciu zo strany lokálneho používateľa, ktorý musí stiahnuť a spustiť špeciálne vytvorený súbor.

Komponent Windows Wi-Fi Driver obsahuje zraniteľnosť CVE-2024-30078, ktorú by útočník nachádzajúci sa v dosahu rádiovej komunikácie prostredníctvom zaslania špeciálne vytvoreného paketu mohol zneužiť na vykonanie škodlivého kódu.

Ostatné zraniteľnosti umožňujúce vykonanie kódu sa nachádzajú v komponentoch Windows Standards-Based Storage Management Service (CVE-2024-30062), Microsoft Event Trace Log File Parsing (CVE-2024-30072), Windows Distributed File System (CVE-2024-30063) a Microsoft Speech Application Programming Interface (CVE-2024-30097). Zneužitie týchto zraniteľností vyžaduje interakciu zo strany používateľa.

Ostatné zraniteľnosti vysokej závažnosti umožňujú eskaláciu privilégií, zneprístupnenie služby 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
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30062
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30063
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30072
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30077
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30078
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30094
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30095

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30097

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 jún bezpečnostné aktualizácie, ktoré opravujú 5 vysoko závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Zraniteľnosť CVE-2024-30103 v Microsoft Outlook umožňuje obídenie blacklist v registroch Outlook a vzdialený autentifikovaný útočník by ju mohol zneužiť na vykonanie škodlivého kódu na úrovni používateľských oprávnení obete. Jedná sa o tzv. **zero-click** zraniteľnosť, ktorá nevyžaduje priamo interakciu s obsahom e-mailu a k jej zneužitiu dochádza pri vygenerovaní náhľadu e-mailu. Bezpečnostní výskumníci plánujú v auguste zverejniť aj proof-of-concept kód demonštrujúci spôsob zneužitia zraniteľnosti.

Zraniteľnosti v produktoch Microsoft SharePoint Server (CVE-2024-30100) a Microsoft Office (CVE-2024-30101, CVE-2024-30102 a CVE-2024-30104) spočívajúce v použití odalokovaného miesta v pamäti a nesprávnom vyhodnocovaní odkazov pred prístupom k súborom by vzdialený útočník mohol zneužiť na vykonanie škodlivého kódu. Zneužitie zraniteľností vyžaduje interakciu zo strany obete, ktorá musí stiahnuť a otvoriť špeciálne vytvorený súbor alebo otvoriť a interagovať s obsahom škodlivej e-mailovej správy.

Zraniteľné systémy:

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
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 Outlook 2016 (32-bit edition)
Microsoft Outlook 2016 (64-bit edition)
Microsoft SharePoint Enterprise 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-2024-30100
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30101
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30102
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30103
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30104
https://blog.morphisec.com/cve-2024-30103-microsoft-outlook-vulnerability

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 jún neopravila ani jednu kritickú alebo vysoko závažnú zraniteľnosť v prehliadači Microsoft Edge.

Zdroje:

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

Mozilla Firefox

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

Zraniteľnosti s označením CVE-2024-5700 (línie Firefox a Firefox ESR) a CVE-2024-5701 (Firefox) možno zneužiť na poškodenie obsahu pamäte a následné vykonanie škodlivého kódu alebo zneprístupnenie služby.

CVE-2024-5688 v línii Firefox a Firefox ESR taktiež umožňuje vykonanie škodlivého kódu alebo zneprístupnenie služby.

Sieťová vrstva prehliadača Firefox ESR obsahuje zraniteľnosť CVE-2024-5702, ktorá spočíva v použití odalokovaného miesta v pamäti a možno ju zneužiť na zneprístupnenie služby.

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

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 127
Mozilla Firefox ESR verzie staršej ako 115.12

Odporúčania:

Odporúčame aktualizovať Firefox na verziu 127 a Firefox ESR na verziu 115.12.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-25/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-26/
https://exchange.xforce.ibmcloud.com/vulnerabilities/294392
https://exchange.xforce.ibmcloud.com/vulnerabilities/294377
https://exchange.xforce.ibmcloud.com/vulnerabilities/294383
https://exchange.xforce.ibmcloud.com/vulnerabilities/294382

Google Chrome

V mesiaci jún spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili celkom 17 vysoko závažných zraniteľností.

Zraniteľnosti s označením CVE-2024-5830, CVE-2024-5833, CVE-2024-5837, CVE-2024-5838 a CVE-2024-6100 v komponente V8 spočívajú v nesprávnej interpretácii typu premennej a možno ju zneužiť na vzdialené vykonanie škodlivého kódu.

Komponenty Dawn (CVE-2024-5831, CVE-2024-5832, CVE-2024-6103, CVE-2024-6290, CVE-2024-6292, CVE-2024-6293) a Swiftshader (CVE-2024-6291) obsahujú zraniteľnosti, ktoré možno prostredníctvom použitia odalokovaného miesta v pamäti zneužiť na vykonanie škodlivého kódu.

Ostatné zraniteľnosti nachádzajúce sa v komponentoch Dawn (CVE-2024-5834, CVE-2024-6102), Tab Groups (CVE-2024-5835), DevTools (CVE-2024-5836) a WebAssembly (CVE-2024-6101) možno zneužiť na obídenie bezpečnostných prvkov, zneprístupnenie služby alebo vykonanie škodlivého 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 126.0.6478.126/127
Google Chrome pre Linux verzie staršej ako 126.0.6478.126

Odporúčania:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 126.0.6478.126/127 a pre Linux aspoň na verziu 126.0.6478.126.

Zdroje:

https://chromereleases.googleblog.com/2024
https://chromereleases.googleblog.com/2024/06/stable-channel-update-for-desktop_24.html
https://chromereleases.googleblog.com/2024/06/stable-channel-update-for-desktop_18.html
https://chromereleases.googleblog.com/2024/06/stable-channel-update-for-desktop_13.html
https://chromereleases.googleblog.com/2024/06/stable-channel-update-for-desktop.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/294405
https://exchange.xforce.ibmcloud.com/vulnerabilities/294410
https://exchange.xforce.ibmcloud.com/vulnerabilities/294413
https://exchange.xforce.ibmcloud.com/vulnerabilities/294406
https://exchange.xforce.ibmcloud.com/vulnerabilities/294463
https://exchange.xforce.ibmcloud.com/vulnerabilities/294411
https://exchange.xforce.ibmcloud.com/vulnerabilities/294464
https://exchange.xforce.ibmcloud.com/vulnerabilities/294407
https://exchange.xforce.ibmcloud.com/vulnerabilities/294408
https://exchange.xforce.ibmcloud.com/vulnerabilities/295055
https://exchange.xforce.ibmcloud.com/vulnerabilities/295056
https://exchange.xforce.ibmcloud.com/vulnerabilities/295057

https://exchange.xforce.ibmcloud.com/vulnerabilities/295058
https://exchange.xforce.ibmcloud.com/vulnerabilities/295547
https://exchange.xforce.ibmcloud.com/vulnerabilities/295548
https://exchange.xforce.ibmcloud.com/vulnerabilities/295549
https://exchange.xforce.ibmcloud.com/vulnerabilities/295550

4. Adobe Acrobat a Reader

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

Zdroje:

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

5. Frameworky

Microsoft .NET Framework

V mesiaci jún spoločnosť Microsoft opravila 2 vysoko závažné zraniteľnosti vo frameworku .NET.

Zraniteľnosť s označením CVE-2024-35252 v Azure Storage Movement Client Library by vzdialený neautentifikovaný útočník prostredníctvom zaslania špeciálne vytvorenej požiadavky mohol zneužiť na zneprístupnenie služby.

Azure Identity Libraries a Microsoft Authentication Library obsahujú bezpečnostnú zraniteľnosť CVE-2024-35255, ktorú by lokálny autentifikovaný útočník mohol zneužiť na eskaláciu privilégií a následné získanie neoprávneného prístupu k obsahu systémových súborov vyžadujúcich oprávnenia úrovne SYSTEM.

Zraniteľné systémy:

Azure Identity Library for .NET
Azure Storage Movement Client Library for .NET
Microsoft Authentication Library (MSAL) for .NET

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-2024-35252
https://exchange.xforce.ibmcloud.com/vulnerabilities/294006

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35255

Oracle Java

Veľká sada opráv je plánovaná na 16. júla 2024.

6. Iné závažné zraniteľnosti

Polyfill.io – z bežnej webovej knižnice malvér

Po odkúpení domény Polyfill.io, ktorá poskytuje knižnicu pre webové aplikácie polyfill.js, sa zistilo, že nový majiteľ upravil funkcionalitu skriptu tak, aby presmerovával požívateľov na škodlivé webstránky. Odporúčame prestať danú knižnicu používať, alebo nahradiť jej zdroj dôveryhodným zdrojom. **Viac informácií na stránke.**

Kritické bezpečnostné zraniteľnosti vo VMware vCenter Server

Spoločnosť BROADCOM vydala bezpečnostné aktualizácie, ktoré opravujú 3 bezpečnostné zraniteľnosti v produkte VMware vCenter Server. Z nich 2 sú označené ako kritické. Zraniteľnosti možno zneužiť na eskaláciu privilégií a vzdialené vykonanie kódu. **Viac informácií na stránke.**

Aktívne zneužívaná zraniteľnosť umožňuje získanie obsahu súborov zo SolarWinds Serv-U

Spoločnosť SolarWinds vydala bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú zraniteľnosť v platforme na prenos súborov Serv-U. Zraniteľnosť umožňujúcu prechádzanie adresárov možno zneužiť na čítanie obsahu súborov na hostiteľskom systéme. **Viac informácií na stránke.**

Kritická zraniteľnosť PHP zneužívaná na šírenie ransomvéru

Vývojári skriptovacieho jazyka PHP vydali bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť. Chyba súvisí s konverziou kódovania znakov cez funkciu Windows Best-Fit a prostredníctvom injekcie príkazov ju možno zneužiť na vzdialené vykonanie kódu. Zraniteľnosť je v súčasnosti aktívne zneužívaná na šírenie ransomvéru TellYouThePass. **Viac informácií na stránke.**

Microsoft v rámci júnového Patch Tuesday opravil kritickú zraniteľnosť v MSMQ

Spoločnosť Microsoft vydala v júni 2024 balík opráv pre portfólio svojich produktov opravujúci 51 zraniteľností, z ktorých 18 umožňuje vzdialené vykonávanie kódu. Kritická bezpečnostná zraniteľnosť sa nachádza v produkte Microsoft Message Queuing. **Viac informácií na stránke.**

Zraniteľnosti v produktoch Veeam

Spoločnosť Veeam vydala bezpečnostné aktualizácie na svoje produkty Backup & Replication, Agent for Windows a Service Provider Console, ktoré opravujú viacero zraniteľností umožňujúcich obchádzanie bezpečnostných prvkov, eskaláciu privilégií alebo vzdialené vykonanie kódu. **Viac informácií na stránke.**

Grafické procesory ARM Mali majú aktívne zneužívanú zraniteľnosť

Aktívne zneužívaná zraniteľnosť ovládača grafických procesorov ARM Mali Valhall a Bifrost umožňuje lokálnemu útočníkovi bez oprávnení získať prístup k dealokovanej pamäti. Zraniteľnosť možno zneužiť na vykonanie kódu alebo získanie neoprávneného prístupu k citlivým údajom. **Viac informácií na stránke.**