Mesačný prehľad kritických zraniteľností júl 2023

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci júl 7 kritických a 96 vysoko závažných zraniteľností.

Kritická zraniteľnosť CVE-2023-32057 sa nachádza v službe Windows Message Queuing (MSMQ). Služba MSMQ systému Windows musí byť povolená, aby mohlo dôjsť k zneužitiu tejto zraniteľnosti. Útočník môže vzdialene vykonávať kód na strane servera odoslaním špeciálne upraveného MSMQ paketu. Microsoft na zmiernenie zraniteľnosti odporúča službu MSMQ vypnúť. Či je služba aktívna môžete skontrolovať v aktívnych procesoch a či zariadenie počúva na porte TCP 1801.

Zraniteľnosť CVE-2023-35297 sa nachádza v protokole Pragmatic General Multicast (PGM). Tento útok je obmedzený na systémy pripojené k rovnakej sieti, v akej sa nachádza útočník.

Neautentifikovaný útočník by mohol zneužiť zraniteľnosť CVE-2023-35315 odoslaním špeciálne vytvorenej požiadavky na Windows Server, konfigurovaný ako Layer-2 Bridge. Zraniteľnosť umožňuje útočníkovi vzdialené vykonávanie kódu. Pre jej úspešné zneužitie musí útočník získať prístup k lokálnej sieti, kde sa nachádza zraniteľný Windows Server, a potom má možnosť pokračovania v útoku.

CVE-2023-35352 umožňuje útočníkovi obísť overenie certifikátu alebo súkromného kľúča pri vytváraní relácie služby vzdialenej pracovnej plochy (remote desktop protocol).

Zraniteľnosti CVE-2023-35365, CVE-2023-35366 a CVE-2023-35367 sa nachádzajú v službe operačného systému Routing and Remote Access Service (RRAS) a umožňujú vzdialené vykonávanie kódu. Pre zneužitie týchto zraniteľností by útočník musel poslať špeciálne vytvorené pakety na server, ktorý je nakonfigurovaný s bežiacou službou RRAS.

Zraniteľnosti vysokej závažnosti umožňujú vzdialené vykonávanie kódu, obchádzanie bezpečnostných prvkov a eskaláciu oprávnení. Zneužitie niektorých z nich môže viesť k úniku informácií a vyvolaniu nedostupnosti služby, či umožniť predstierať cudziu identitu.

Zraniteľné systémy:

Raw Image Extension
VP9 Video Extensions
Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
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 11 version 21H2 for ARM64-based Systems
Windows 11 version 21H2 for x64-based Systems
Windows 11 Version 22H2 for ARM64-based Systems
Windows 11 Version 22H2 for x64-based Systems
Windows Admin Center
Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
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)

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-2023-32057
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35297
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35315
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35352
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35365
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35366
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35367

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci júl 2 kritické a 16 vysoko závažných zraniteľností.

Kritické zraniteľnosti CVE-2023-33157 a CVE-2023-33160 sa nachádzajú v Microsoft SharePoint a SharePoint Server a umožňujú útočníkovi pristupovať k informáciám obete a vykonávať zmeny. Úspešné zneužitie, môže tiež potenciálne spôsobiť výpadok v postihnutom

prostredí. Druhá zraniteľnosť vyžaduje, aby používateľ pristupoval k citlivému API rozhraniu na postihnutých verziách SharePointu s osobitne naformátovaným vstupom, čo môže viesť k možnej vzdialenej exekúcii kódu na serveri SharePoint. Útočník musí získať autentifikáciu na cieľovom webovom mieste aspoň ako registrovaný užívateľ.

Zraniteľnosti vysokej závažnosti umožňujú vzdialené vykonávanie kódu, obchádzanie bezpečnostných prvkov a eskaláciu oprávnení. Zneužitie niektorých z nich môže viesť k úniku informácií, či umožniť útočníkom predstierať cudziu identitu.

Zraniteľné systémy:

Paint 3D
Microsoft Word 2016 (64-bit edition)
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2013 Service Pack 1 (64-bit editions)
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 RT Service Pack 1
Microsoft SharePoint Server Subscription Edition
Microsoft SharePoint Server 2019
Microsoft SharePoint Enterprise Server 2016
Microsoft Outlook 2016 (64-bit edition)
Microsoft Outlook 2016 (32-bit edition)
Microsoft Outlook 2013 RT Service Pack 1
Microsoft Outlook 2013 (64-bit editions)
Microsoft Outlook 2013 (32-bit editions)
Microsoft Office for Universal
Microsoft Office Online Server
Microsoft Office LTSC for Mac 2021
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office 2019 for Mac
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Click-to-Run (C2R) for 64-bit editions
Microsoft Office 2013 Click-to-Run (C2R) for 32-bit editions
Microsoft Excel 2016 (64-bit edition)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 RT Service Pack 1
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft 365 Apps for Enterprise for 32-bit Systems

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-2023-33157
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33160

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. Pre zvyšné operačné systémy, kde je prehliadač ešte podporovaný, nevydala v mesiaci júl žiadne opravy kritických a závažných zraniteľností.

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

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance

Microsoft Edge

Spoločnosť Microsoft v mesiaci júl opravila v prehliadači Microsoft Edge jednu závažnú zraniteľnosť.

Zraniteľnosť CVE-2023-36887 umožňuje útočníkovi získať schopnosť vzdialene vykonať kód (RCE). Prihlásený útočník ju môže zneužiť spustením špeciálne vytvoreného súboru na zraniteľnom systéme alebo presvedčiť obeť, aby takýto súbor spustila.

Zraniteľné systémy:
Microsoft Edge (Chromium-based) build 114.0.1823.82

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-2023-36887

Mozilla Firefox

V mesiaci júl bolo opravených 5 vysoko závažných zraniteľností v línii Firefox a Firefox ESR.

Zraniteľnosť CVE-2023-3600 spočíva v spôsobe spracovania škodlivých údajov z prichádzajúcich e-mailov. To umožňuje útočníkovi spustiť ľubovoľný kód. Útočník využije dealokované miesto pamäte počas životného cyklu pracovníka pri spracovaní obsahu HTML. Zraniteľnosť sa nachádza v prehliadači Firefox < 115.0.2, Firefox ESR < 115.0.2 a Thunderbird < 115.0.1.

Zraniteľnosť CVE-2023-37201 ovplyvňuje funkčnosť komponentu WebRTC. Útočníkovi umožňuje použiť dealokované miesto pamäte pri vytváraní spojenia WebRTC pomocou HTTPS.

Zraniteľnosť CVE-2023-37202 vo wrapperi v SpiderMonkey pre skriptované proxy by mohla spôsobiť ukladanie objektov z iných oddielov do hlavného oddielu, čo by viedlo k použitiu pamäte po jej dealokácii.

Zraniteľnosti CVE-2023-37211 a CVE-2023-37212 umožňujú útočníkom vykonávať ľubovoľný kód kvôli chybe poškodeniu pamäte. Zraniteľnosti sa nachádzajú v prehliadači Firefox 114, Firefox ESR 102.12 a poštovom klientovi Thunderbird 102.12.

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 115.0.2
Mozilla Firefox ESR verzie staršej ako 115.0.2

Odporúčania:

Odporúčame aktualizáciu Mozilla Firefox na verziu 115.0.2 a Mozilla Firefox ESR na verziu 115.02

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-22/
https://csirt.telconet.net/comunicacion/noticias-seguridad/nueva-vulnerabildiad-de-tipo-rce-en-mozilla-thunderbird/

https://www.mozilla.org/en-US/security/advisories/mfsa2023-23/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-26/

Google Chrome

V mesiaci júl bola vydaná oprava 4 vysoko závažných zraniteľností prehliadača Google Chrome. Dve z nich sú aktívne zneužívané.

Zraniteľnosti CVE-2023-3727, CVE-2023-3728 a CVE-2023-3730 umožňujú použiť dealokované miesto pamäte v komponentoch WebRTC a Tab Groups.

CVE-2023-3732 umožňuje pristupovať k pamäti mimo povolené hodnoty v Mojo.

Zraniteľné systémy:

Google Chrome pre Windows verzie staršej ako 115.0.5790.98/99 a Linux a Mac verzie staršej ako 115.0.5790.98.

Odporúčania:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 115.0.5790.98/99 a Linux aspoň na verziu 115.0.5790.98.

Zdroje:

https://chromereleases.googleblog.com/2023/07/
https://chromereleases.googleblog.com/2023/07/stable-channel-update-for-desktop.html

4. Adobe Acrobat a Reader

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

Zdroje:

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

5. Frameworky

Microsoft .NET Framework

V mesiaci júl spoločnosť Microsoft opravila 2 kritické zraniteľnosti vo frameworku .NET.

Úspešné zneužitie zraniteľností CVE-2023-33127 a CVE-2023-33170 vyžaduje, aby útočník úspešne zneužil súbeh a taktiež vykonal dodatočné kroky pred samotným zneužitím na prípravu cieľového prostredia. Útočník by mohol zneužiť prvú zraniteľnosť pomocou .NET diagnostického servera za účelom eskalácie oprávnení a druhú pre obídenie bezpečnostných prvkov.

Zraniteľné systémy:
.NET 6.0
.NET 7.0

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-2023-33127
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33170

Oracle Java

V mesiaci júl vydala spoločnosť Oracle veľkú sadu opráv v platforme Java SE a GraalVM Enterprise Edition. Žiadna z nich nebola kritická ani vysoko závažná.

Zdroje:
https://www.oracle.com/security-alerts/
https://www.oracle.com/security-alerts/cpujul2023.html#AppendixJAVA

6. Iné závažné zraniteľnosti

Zero-day zraniteľnosti v zariadeniach od spoločnosti Apple

Spoločnosť Apple vydala opravu zraniteľností CVE-2023-38606 a CVE-2023-37450, ktoré môže viesť ku vzdialenému vykonávaniu kódu. Chyby sa týkajú zariadení so systémom iOS, macOS, watchOS a webového prehliadača Safari. CVE-2023-37450 sa vyskytuje vo frameworku WebKit. Používateľom je odporúčané nainštalovať si najnovšie dostupné aktualizácie. Viac informácií na stránke.

Kritická zraniteľnosť v Technicolor DSL TG670 routri s verziou firmvéru 10.5.N.9.

Nezávislý bezpečnostný výskumník identifikoval prítomnosť viacerých servisných administratívnych účtov priamo v zdrojovom kóde routeru Technicolor DSL TG670 s verziou firmvéru 10.5.N.9. Zraniteľnosť umožňuje vzdialenému útočníkovi využiť prihlasovacie údaje nachádzajúce sa v zdrojovom kóde routera na získanie vzdialeného administratívneho prístupu k routeru prostredníctvom protokolov HTTP, SSH alebo TELNET a následne upravovať jeho administratívne nastavenia. Viac informácií na stránke.

Zraniteľnosť zariadení Ubiquiti EdgeRouter a AirCube

Spoločnosť Ubiquiti vydala správu o prítomnosti zraniteľnosti typu RCE a DoS vo svojich zariadeniach EdgeRouter a AirCube. Zneužitím zraniteľnosti by potenciálny útočník mohol na zariadeniach vykonať škodlivý kód, čím by mohol zamedziť korektnému fungovaniu zariadení, prípadne ich použiť na šírenie a vykonávanie ďalšej škodlivej činnosti. Zraniteľnosť bola na oboch zariadeniach odstránená pomocou bezpečnostných aktualizácií vo verziách EdgeRouter 2.0.9-hotfix.7 a AirCube 2.8.9. Viac informácií na stránke.

Zraniteľnosť v Zimbra Collaboration Suite umožňuje XSS

Spoločnosť Zimbra opraví vo svojom produkte Collaboration Suite zaávažnú aktívne zneužívanú zraniteľnosť, ktorá umožňuje kvôli chýbajúcej sanitizácii používateľských vstupov vykonávať útoky typu XSS. Viac informácií na stránke.

Kritická zraniteľnosť v produkte SAP Business Client a v produktoch SAP ECC, SAP S/4HANA

Spoločnosť SAP opravila viacero zraniteľností vo svojich produktoch. Medzi najzávažnejšie opravené zraniteľnosti patrí kritická zraniteľnosť v rámci produktu SAP Business Client a kritická zraniteľnosť v produkte SAP ECC, SAP S/4HANA (IS-OIL). Zneužitie zraniteľnosti CVE-2023-33299 môže viesť k injekcii príkazov pre operačný systém, čo môže viesť k narušeniu dostupnosti, integrity a dôvernosti údajov. Celkovo spoločnosť SAP zverejnila 16 bezpečnostných poznámok týkajúcich sa niekoľkých produktov. Viac informácií na stránke.

Kritická zraniteľnosť produktov FortiOS a FortiProxy

Spoločnosť Fortinet oznámila prítomnosť kritickej bezpečnostnej zraniteľnosti v produktoch FortiOS a FortiProxy. Zraniteľnosť umožňuje potenciálnemu vzdialenému útočníkovi vykonať na cieľovom zariadení ľubovoľný kód alebo príkazy prostredníctvom špecificky vytvorených paketov a môže viesť k celkovej kompromitácii zariadenia. Zraniteľnosť bola odstránená vo

verziách FortiOS 7.2.4 a vyššie, 7.0.11 a vyššie a vo verziách FortiProxy 7.2.3 a vyššie a 7.0.10 a vyššie. Viac informácií na stránke.