Mesačný prehľad kritických zraniteľností
jún 2023

1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci jún 4 kritické a 33 vysoko závažných zraniteľností.

Kritické zraniteľnosti CVE-2023-29363, CVE-2023-32014 a CVE-2023-32015 sa nachádzajú v protokole Pragmatic General Multicast (PGM). Útočníkovi dovoľujú vykonať kód odoslaním špeciálne vytvoreného súboru po sieti, keď je spustená služba Windows Message Queuing (MSMQ). Microsoft na zmiernenie zraniteľnosti odporúča používateľom služby MSMQ využívať základnú konfiguráciu alebo skontrolovať službu na porte TCP 1801.

Zraniteľnosť CVE-2023-32013 sa nachádza vo virtualizačnej platforme Hyper-V a umožňuje vyvolať nedostupnosť služby. Pre úspešné zneužitie tejto zraniteľnosti musí útočník pripraviť cieľové prostredie s cieľom zvýšiť spoľahlivosť zneužitia zraniteľnosti.

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:

Remote Desktop client for Windows Desktop
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 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-2023-29363
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32013
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32014
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32015

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci jún 1 kritickú 10 vysoko závažných zraniteľností.

Kritická zraniteľnosť CVE-2023-29357 umožňuje neautentifikovanému útočníkovi zvýšiť svoje oprávnenia na úroveň administrátora a získať prístup ku JWT autentifikačným tokenom. Útočníkovi dovoľuje zneužiť autentifikačný token pre autentifikáciu a vykonať sieťový útok.

Zranitelnosti CVE-2023-32029, CVE-2023-33131, CVE-2023-33133, CVE-2023-33137 a CVE-2023-33146 umožňujú útočníkovi vzdialene vykonávať kód. Pre zneužitie zraniteľnosti musí obeť otvoriť útočníkom podvrhnutý škodlivý súbor.

CVE-2023-33129 umožňuje autentifikovanému útočníkovi s oprávnením na používanie správy zoznamov v platforme Microsoft SharePoint odoslať špeciálne vytvorenú požiadavku, ktorá môže viesť ku pádu aplikácie.

Útočník, ktorý úspešne zneužije zraniteľnosť CVE-2023-33142, je schopný vytvoriť zoznam alebo knižnicu dokumentov na cieľovom webovom sídle SharePoint a tým ovplyvniť jeho integritu. Útočník by nemohol upravovať ani mazať zoznam alebo knižnicu dokumentov zo sídla SharePoint.

Zraniteľnosť CVE-2023-33140, umožňuje útočníkovi predstierať cudziu identitu v zraniteľnej inštancii Microsoft OneNote pomocou spustenia špeciálne vytvoreného súbor. Pre jej zneužitie je potrebná interakcia zo strany obete so škodlivým URL odkazom.

Útočník by mohol zneužiť zraniteľnosti CVE-2023-33130 a CVE-2023-33132 pre falšovanie svojej identity. K tomu potrebuje presvedčiť obeť, aby klikla na podvrhnutý odkaz obsahujúci špeciálne vytvorený súbor. Útočník môže využiť útok typu Cross-Site Scripting (XSS), vložiť svoj špeciálne vytvorený kód a získať tak citlivé informácie obete alebo meniť vykonávanie DOM (Document Object Model). Útočník musí byť autentifikovaný na cieľovú stránku aspoň ako člen webu.

Zraniteľné systémy:

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
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 2019 for Mac
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 OneNote for Universal
Microsoft Outlook 2013 (32-bit editions)
Microsoft Outlook 2013 (64-bit editions)
Microsoft Outlook 2013 RT Service Pack 1
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-2023-29357
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32029
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33129
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33130
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33131
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33132
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33133
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33137
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33140
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33142
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33146

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 jún 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 jún opravila v prehliadači Microsoft Edge jednu závažnú zraniteľnosť.

Zraniteľnosť CVE-2023-33145 sa nachádza v komponente Webview2 a umožňuje útočníkovi získať citlivé údaje z webstránky. Na to potrebuje presmerovať obeť na škodlivú webstránku.

Zraniteľné systémy:
Microsoft Edge (Chromium-based) build 111.0.1661.41

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-2023-24892

Mozilla Firefox

V mesiaci jún boli opravené 3 vysoko závažné zraniteľnosti.

Zraniteľnosť CVE-2023-34414 umožňuje útočníkovi autentifikovať chybný certifikát za dôveryhodný. Stránka s chybovou hláškou pre stránky s neplatnými TLS certifikátmi nemala nastavenú aktiváciu potvrdzovacieho tlačidla s oneskorením, ktoré Firefox používa na ochranu pred útokmi využívajúcimi oneskorenie ľudskej odozvy. Pri presmerovaní na stránky s upozornením na chybný certifikát a so zaneprázdneným vykresľovacím nástrojom môže byť kliknutie obete zaznamenané ešte pred vykreslením hlásenia na obrazovke.

Označenia CVE-2023-34416 (Firefox a Firefox ESR) a CVE-2023-34417 (Firefox) pokrývajú sadu zraniteľností ovplyvňujúcich bezpečnosť pamäte, ktoré môžu viesť ku poškodeniu pamäte alebo možnosti vykonávať kód. Vývojári z prostredia Mozilla a členovia komunity Gabriele Svelto, Andrew McCreight, tím Mozilla Fuzzing Team, Sean Feng a Sebastian Hengst hlásili chyby v bezpečnosti pamäte vo verzii Firefox 113 a Firefox ESR 102.11.

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 114
Mozilla Firefox ESR verzie staršej ako 102.12

Odporúčania:

Odporúčame aktualizáciu Mozilla Firefox na verziu 114 a Mozilla Firefox ESR na verziu 102.12

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-19/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-20/

Google Chrome

V mesiaci jún bola vydaná oprava 1 kritickej a 7 vysoko závažných zraniteľností prehliadača Google Chrome.

Kritická zraniteľnosť CVE-2023-3214 súvisiaca s použitím dealokovaného miesta v pamäti sa nachádza v softvéri Chromium Open Source Software (OSS), ktorý využíva aj prehliadač Microsoft Edge (založený na Chromium). Chyba sa vyskytuje v komponente Autofill pri automatickom vkladaní citlivých dát pri platbách.

Zraniteľnosti CVE-2023-3079, CVE-2023-3216 a CVE-2023-3420 súvisia s neoverením typu premennej v komponente V8. CVE-2023-3215, CVE-2023-3217, CVE-2023-3421 a CVE-2023-3422 sa nachádzajú v komponentoch WebRTC, WebXR, Media, Guest View v prehliadači Google Chrome. Tieto zraniteľnosti umožňujú pomocou škodlivej HTML stránky zneužiť dealokované miesto v pamäti na halde.

Zraniteľné systémy:

Google Chrome pre Windows, Mac a Linux verzie staršej ako 114.0.5735.198/199.

Odporúčania:

Odporúčame aktualizáciu prehliadača Chrome pre Windows, Mac a Linux aspoň na verziu 114.0.5735.198/199.

Zdroje:

https://chromereleases.googleblog.com/2023/06/
https://chromereleases.googleblog.com/2023/06/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2023/06/stable-channel-update-for-desktop_13.html
https://chromereleases.googleblog.com/2023/06/stable-channel-update-for-desktop_26.html

4. Adobe Acrobat a Reader

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

Zdroje:

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

5. Frameworky

Microsoft .NET Framework

V mesiaci jún spoločnosť Microsoft opravila 1 kritickú a 5 vysoko závažných zraniteľností vo frameworku .NET.

Kritická zraniteľnosť CVE-2023-24897 umožňuje vzdialené vykonávanie kódu. Útočník pre jej zneužitie musí presvedčiť obeť, aby interagovala s podvrhnutým škodlivým súborom.

Vysoko závažné zraniteľnosti CVE-2023-32030 a CVE-2023-29331 umožňujú vyvolanie nedostupnosti služby, CVE-2023-29326 a CVE-2023-24895 umožňujú vzdialené vykonávanie kódu a CVE-2023-33135 môže viesť k eskalácii oprávnení útočníka.

Zraniteľné systémy:

.NET 6.0
.NET 7.0
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.0 Service Pack 2/3.5/3.5.1
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2/4.8/4.8.1

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-2023-24897

Oracle Java

Najbližšia veľká sada opráv je plánovaná na 18. júla 2023.

Zdroje:

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

6. Iné závažné zraniteľnosti

Kritická zraniteľnosť produktu FortiNAC

Spoločnosť Fortinet opravila kritickú zraniteľnosť typu RCE vo svojom produkte FortiNAC. Produkt sa používa ako bezpečnostný prvok na riadenie prístupu (Network Access Control) v enterprise a IoT sieťach. Potenciálny vzdialený a neautentifikovaný útočník by mohol zneužiť

zraniteľnosť na narušenie integrity infraštruktúry organizácie pomocou vzdialeného vykonávania kódu a príkazov. Zraniteľnosť bola odstránená vo verziách FortiNAC 7.2.2, 9.1.10, 9.2.8, 9.4.3 alebo novších. Viac informácií na stránke.

Nesprávna konfigurácia Microsoft OAuth v cloudovej službe Azure AD

Spoločnosť Microsoft opravila kritickú zraniteľnosť vo svojom e-mailovom riešení Outlook. Jej zneužitie umožňuje získať na diaľku zvýšené oprávnenia v zraniteľnom systéme bez interakcie obete. Zraniteľnosť už takmer rok aktívne zneužívajú ruskí štátni aktéri zo skupiny APT28. Viac informácií na stránke.

Viacero zraniteľností v Splunk Enterprise

Spoločnosť Splunk vydala bezpečnostné aktualizácie na opravu 5 závažných zraniteľností v softvéri Splunk Enterprise. Tieto zraniteľnosti by mohli viesť k eskalácii oprávnení, prístupu cez adresár (path traversal), lokálnej eskalácii oprávnení, odmietnutia poskytovania služieb/nedostupnosť služieb DDoS (denial of service) alebo rozdeľovaniu HTTP odozvy (HTTP response splitting). Viac informácií na stránke.

Kritická zraniteľnosť FortiGate SSL VPN

Spoločnosť Fortinet opravila kritickú zraniteľnosť svojho zariadenia FortiGate (NGFW). Kritická zraniteľnosť umožňuje neautentifikovanému útočníkovi vzdialené vykonávanie kódu a príkazov. Používatelia dotknutých bezpečnostných produktov by mali bezodkladne aktualizovať ich firmvér. Pokiaľ to nie je možné, napríklad z dôvodu vypršania podpory zariadenia, odporúča sa zariadenie úplne vypnúť vzhľadom k mimoriadnemu bezpečnostnému riziku. Viac informácií na stránke.

Zraniteľnosť KeePass umožňuje získať hlavné heslo z pamäte

Spoločnosť KeePass vydala verziu KeePass 2.54, ktorá opravuje kritickú zraniteľnosť ohrozujúcu bezpečnosť citlivých dát používateľov aplikácie. Útočník má možnosť získať dáta z neošetreného textového poľa „SecureTextBoxEx“, ktoré sa používa pre zadávanie hlavného hesla, ako aj pre úpravu hesiel. Zneužitie predmetnej zraniteľnosti umožňuje útočníkovi extrahovať citlivé údaje z výpisu pamäte aplikácie. Viac informácií na stránke.