Mesačný prehľad kritických zraniteľností apríl 2023

1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci apríl 7 kritických a 70 vysoko závažných zraniteľností.

Všetky opravené kritické zraniteľnosti umožňujú útočníkom vzdialene vykonávať kód.

Kritická zraniteľnosť CVE-2023-21554 sa nachádza v službe Windows Message Queuing (MSMQ) a dostala pomenovanie QueueJumper. Útočník môže vzdialene vykonávať kód na strane servera odoslaním špeciálne upraveného MSMQ paketu.

Zraniteľnosti CVE-2023-28219, CVE-2023-28220 a CVE-2023-28232 sa nachádzajú v protokole PPTP. Prvé dve dovoľujú neautentifikovanému útočníkovi vykonávať kód na serveri RAS odoslaním špeciálne vytvorenej požiadavky na pripojenie. Posledná umožňuje vykonať kód po pripojení klienta s operačným systémom Windows ku škodlivému serveru.

CVE-2023-28231 sa nachádza v službe DHCP Server. Neautentifikovanému útočníkovi s prístupom do siete dovoľuje vykonať kód odoslaním špeciálne vytvorenej požiadavky službe DHCP.

CVE-2023-28250 sa nachádza v protokole Pragmatic General Multicast (PGM). Pre jej zneužitie je potrebné, aby bola povolená služba MSMQ. Útočníkovi dovoľuje vykonať kód odoslaním špeciálne vytvoreného súboru po sieti.

CVE-2023-28291 sa nachádza v komponente Raw Image Extension. Prihlásený útočník ju môže zneužiť spustením špeciálne vytvorenej aplikácie na zraniteľnom systéme alebo presvedčiť obeť, aby takúto aplikáciu spustila.

Zraniteľnosti vysokej závažnosti umožňujú vzdialené vykonávanie kódu, obchádzanie bezpečnostných prvkov, predstieranie cudzej identity a eskaláciu oprávnení. Zneužitie niektorých z nich môže viesť k úniku informácií a vyvolaniu nedostupnosti služby.

Zraniteľné systémy:

Raw Image Extension
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 20H2 for 32-bit Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 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-2023-21554
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28219
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28220
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28231
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28232
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28250
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28291

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci apríl 5 vysoko závažných zraniteľností.

Zraniteľnosti CVE-2023-28285, CVE-2023-28287, CVE-2023-28295 a CVE-2023-28311 umožňujú vzdialene vykonávať kód.

Zraniteľnosť CVE-2023-28288 môže útočník zneužiť pri predstieraní cudzej identity.

Zraniteľné systémy:

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
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 Publisher 2013 Service Pack 1 (32-bit editions)
Microsoft Publisher 2013 Service Pack 1 (64-bit editions)
Microsoft Publisher 2013 Service Pack 1 RT
Microsoft Publisher 2016 (32-bit edition)
Microsoft Publisher 2016 (64-bit edition)
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
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

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 apríl 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 apríl opravila v prehliadači Microsoft Edge jednu kritickú zero-day zraniteľnosť.

Zraniteľnosť CVE-2023-2033 sa nachádza v komponente V8 a súvisí s neoverením typu premennej. Útočníkom umožňuje pomocou škodlivej HTML stránky zneužiť poškodenie pamäte na halde. Zraniteľnosť je aktívne zneužívaná.

Zraniteľné systémy:

Microsoft Edge (Chromium-based) build 112.0.1722.48

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-2023-2033
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2033

Mozilla Firefox

V mesiaci apríl bolo opravených 10 vysoko závažných zraniteľností v línii Firefox a Firefox ESR.

Zraniteľnosť CVE-2023-29531 vo Firefox pre macOS umožňuje pristupovať k pamäti mimo povolené hodnoty pomocou WebGL API volaní. Jej zneužitie vedie k poškodeniu pamäti a potenciálnej možnosti zneužitia tohto stavu.

CVE-2023-29532 vo Firefox pre Windows umožňuje kvôli nedostatočnej kontrole útočníkovi s lokálnym prístupom ku zraniteľnému systému obísť zabezpečenie Mozilla Maintenance Service a nainštalovať nepodpísaný aktualizačný súbor umiestnený na škodlivom SMB serveri.

CVE-2023-29533 umožňuje ukryť oznámenie o prepnutí do režimu plnej obrazovky. Útočník by chybu mohol zneužiť na zmätenie obete.

CVE-2023-29534 vo Firefox a Focus pre Android umožňuje ukryť oznámenie o prepnutí do režimu plnej obrazovky. Útočník by chybu mohol zneužiť na zmätenie obete.

CVE-2023-29535 súvisí s možnosťou prístupu ku weak mapám v algoritme garbage collector a môže viesť k potenciálne zneužiteľnému poškodeniu pamäte.

CVE-2023-29536 umožňuje útočníkovi spôsobiť, že manažér pamäte JavaScript nevhodne uvoľní ukazovateľ smerujúci na časť pamäte, ktorú kontroluje.

Zraniteľnosť CVE-2023-29537 predstavuje viacero súbehov v inicializácii fontov, ktoré môžu umožniť vykonávanie kódu.

CVE-2023-1999 v knižnici libwebp súvisí s pokusom uvoľniť už uvoľnenú pamäť (double-free) a môže viesť k jej potenciálne zneužiteľnému poškodeniu.

Označenia CVE-2023-29550 (Firefox a Firefox ESR) a CVE-2023-29551 (Firefox) pokrývajú sadu zraniteľností ovplyvňujúcich bezpečnosť pamäte, ktoré môžu viesť ku poškodeniu pamäte alebo možnosti vykonávať kód.

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 112

Mozilla Firefox ESR verzie staršej ako 102.10

Odporúčania:

Odporúčame aktualizáciu Mozilla Firefox na verziu 112 a Mozilla Firefox ESR na verziu 102.10

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-13/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-14/

Google Chrome

V mesiaci apríl bola vydaná oprava 7 vysoko závažných zraniteľností prehliadača Google Chrome. Dve z nich sú aktívne zneužívané.

Zraniteľnosť CVE-2023-1810 súvisí s pretečením medzipamäte na halde v komponente Visuals.

CVE-2023-1811 a CVE-2023-2135 umožňujú použiť dealokované miesto v pamäti v komponentoch Frames a DevTools.

CVE-2023-2033 je zero-day zraniteľnosť súvisiaca so zámenou typu premennej v komponente V8.

Zraniteľnosti CVE-2023-2133 a CVE-2023-2134 v komponente Service Worker API dovoľujú čítať mimo povolené hodnoty v pamäti.

CVE-2023-2136 je zero-day zraniteľnosť súvisiaca s pretečením celočíselnej premennej v komponente Skia.

Zraniteľné systémy:

Google Chrome pre Windows a Mac verzie staršej ako 112.0.5615.137/138 a Linux verzie staršej ako 112.0.5615.165.

Odporúčania:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 112.0.5615.137/138 a Linux aspoň na verziu 112.0.5615.165.

Zdroje:

https://chromereleases.googleblog.com/2023/04/
https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_14.html
https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html

4. Adobe Acrobat a Reader

V produkte Adobe Acrobat a Reader bolo v mesiaci apríl opravených 14 kritických a 2 vysoko závažné zraniteľnosti.

Kritické zraniteľnosti CVE-2023-26395, CVE-2023-26405, CVE-2023-26407, CVE-2023-26417, CVE-2023-26418, CVE-2023-26419, CVE-2023-26420, CVE-2023-26421, CVE-2023-26422, CVE-2023-26423, CVE-2023-26424 a CVE-2023-26425 umožňujú vykonávanie ľubovoľného kódu kvôli podtečeniu celočíselnej premennej, chybe čítania a zápisu do pamäte mimo povolené hodnoty, nevhodnej validácii vstupov a použitiu dealokovaného miesta v pamäti.

Kritické zraniteľnosti CVE-2023-26406 a CVE-2023-26408 umožňujú obchádzať bezpečnostné prvky kvôli nevhodnej kontrole prístupu.

Vysoko závažná zraniteľnosť CVE-2023-26396 môže viesť k eskalácii privilégií kvôli porušeniu princípov bezpečného dizajnu kódu.

Vysoko závažná zraniteľnosť CVE-2023-26397 môžu viesť k úniku obsahu pamäte kvôli chybe umožňujúcej čítanie pamäte mimo povolené hodnoty.

Zraniteľné systémy:

Acrobat DC a Acrobat Reader DC pre Windows a Mac verzie 23.001.20093 a staršie,
Acrobat 2020 a Acrobat Reader 2020 pre Windows a Mac verzie 20.005.30441 a staršie.

Odporúčania:

Odporúčame aktualizáciu aspoň na verziu:
Acrobat DC a Acrobat Reader DC pre Windows a Mac 23.001.20143,
Acrobat 2020 a Acrobat Reader 2020 pre Windows a Mac 20.005.30467.

Zdroje:

https://helpx.adobe.com/security/security-bulletin.html
https://helpx.adobe.com/security/products/acrobat/apsb23-24.html

5. Frameworky

Microsoft .NET Framework

V mesiaci apríl spoločnosť Microsoft opravila jednu kritickú zraniteľnosť vo frameworku .NET.

Kritická zraniteľnosť CVE-2023-28260 umožňuje neautentifikovanému útočníkovi vykonávať kód zneužitím metódy DLL hijacking.

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-2023-28260

Oracle Java

V mesiaci apríl opravila spoločnosť Oracle v platforme Java SE a GraalVM Enterprise Edition jednu vysoko závažnú zraniteľnosť.

Zraniteľnosť CVE-2023-21930 umožňuje neautentifikovanému útočníkovi so sieťovým prístupom prístup a manipuláciu s citlivými a kritickými údajmi. Zraniteľnosť je možné zneužiť aj pomocou API.

Zraniteľné systémy:

Oracle Java SE 8u361, 8u361-perf, 11.0.18, 17.0.6, 20 a GraalVM Enterprise Edition 20.3.9, 21.3.5, 22.3.1

Odporúčania:

Odporúčame aktualizáciu Oracle JavaSE a GraalVM Enterprise Edition na najnovšiu verziu.

Zdroje:

https://www.oracle.com/security-alerts/
https://www.oracle.com/security-alerts/cpuapr2023.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21930

6. Iné závažné zraniteľnosti

Android má dve kritické RCE a jednu zero-day zraniteľnosť

Spoločnosť Google vydala v apríli balík opráv 68 zraniteľností vo svojom systéme Android a jeho komponentoch. Z nich 6 je označených ako kritické. Jedna vysoko závažná zraniteľnosť ovládača GPU Arm Mali je aktívne zneužívaná. Viac informácií na stránke.

VMware vydáva aktualizáciu na opravu kritickej chyby vRealize (Aria)

Používatelia produktu VMware vRealize, po novom Aria Operations for Logs, čelia hrozbe, kedy neautentifikovaný útočník môže jednoduchým spôsobom vzdialene vykonávať ľubovoľný kód s oprávneniami používateľa root. Viac informácií na stránke.