Mesačný prehľad kritických zraniteľností
máj 2023

1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci máj 5 kritických a 22 vysoko závažných zraniteľností.

Všetky opravené kritické zraniteľnosti umožňujú útočníkom vzdialene vykonávať kód.

Zraniteľnosť CVE-2023-24903 sa nachádza v Secure Socket Tunneling protokole (SSTP). Pre jej zneužitie musí neautentifikovaný útočník vytvoriť špeciálnu požiadavku na pripojenie k RAS serveru alebo špeciálne vytvorený SSTP paket SSTP serveru.

CVE-2023-29325 sa nachádza v mechanizme Windows Object Linking and Embedding (OLE). Útočník môže odoslať obeti špeciálne vytvorený e-mail. Zneužitie zraniteľnosti by mohlo útočníkovi umožniť vzdialené vykonávanie kódu, pričom stačí, aby obeť otvorila škodlivý e-mail v aplikácii Outlook alebo Outlook zobrazil náhľad a-mailu.

CVE-2023-24943 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-2023-28283 sa nachádza v protokole LDAP. Neautentifikovaný útočník má možnosť spustiť kód kódu v kontexte služby LDAP prostredníctvom vytvorenia sady volaní LDAP.

Zraniteľnosť CVE-2023-24941 je možné zneužiť prostredníctvom neautentifikovaného volania služby Network File System (NFS), čím môže útočník získať schopnosť vzdialene vykonať kód (RCE).

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.

Zraniteľné systémy:

AV1 Video Extension
Microsoft Remote 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-2023-24903
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24943
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28283
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24941

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci máj 1 kritickú a 7 vysoko závažných zraniteľností.

Kritická zraniteľnosť CVE-2023-24955 umožňuje autentifikovanému útočníkovi v role Site Owner vykonať kód na diaľku na serveri SharePoint.

Zraniteľnosti CVE-2023-29344, CVE-2023-29335, CVE-2023-29333, CVE-2023-24954, CVE-2023-24953 a CVE-2023-24881 umožňujú vzdialene vykonávať kód. Zraniteľnosť CVE-2023-24950 má možnosť úniku hashu NTLM servera.

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 SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Teams
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 Service Pack 1 (64-bit editions)
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit 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://msrc.microsoft.com/update-guide/
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29333
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29344
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24954

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24955
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24950
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24881
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24953
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335

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 máj 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 máj opravila v prehliadači Microsoft Edge jednu závažnú zraniteľnosť.

Zraniteľnosť CVE-2023-29350 umožňuje útočníkovi zvýšiť svoje oprávnenia a úplne kompromitovať zraniteľný prehliadač. Obeť na to musí interagovať so škodlivou URL.

Zraniteľné systémy:

Microsoft Edge (Chromium-based)

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-2023-29350

Mozilla Firefox

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

Útočník by mohol využiť zraniteľnosť CVE-2023-32205, ktorá súvisí so zakrývaním výziev používateľovi vyskakujúcimi oknami, na zmätenie obete (možnosť spoofingu).

Zraniteľnosť CVE-2023-32206, umožňujúca čítanie pamäte mimo povolených hodnôt, môže zapríčiniť pád ovládača RLBox Expat.

CVE-2023-32207 umožňuje útočníkovi získať povolenia od používateľa kvôli chýbajúcemu opozdeniu vo vyskakovacích oznámeniach.

Označenia CVE-2023-32215 (Firefox a Firefox ESR) a CVE-2023-32216 (Firefox) pokrývajú sadu zraniteľností ovplyvňujúcich bezpečnosť pamäte, ktoré môžu viesť ku poškodeniu pamäte alebo možnosti vykonávať kód.

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 113
Mozilla Firefox ESR verzie staršej ako 102.11

Odporúčania:

Odporúčame aktualizáciu Mozilla Firefox na verziu 113 a Mozilla Firefox ESR na verziu 102.11

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-17/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-16/

Google Chrome

V mesiaci máj bola vydaná oprava 1 kritickej a 11 vysoko závažných zraniteľností prehliadača Google Chrome.

Kritická zraniteľnosť CVE-2023-2721 a vysoko závažné zraniteľnosti CVE-2023-2722, CVE-2023-2723, CVE-2023-2725, CVE-2023-2930, CVE-2023-2931, CVE-2023-2932 a CVE-2023-2933 umožňujú použiť dealokované miesto pamäte v komponentoch Navigation, Autofill UI, DevTools, Guest View, Extensions a PDF.

Vysoko závažná zraniteľnosť CVE-2023-2929 v komponente Swiftshader umožňuje zapisovať do pamäte mimo povolené hodnoty a CVE-2023-2934 v Mojo umožňuje pristupovať k pamäti mimo povolené hodnoty.

Zraniteľnosti CVE-2023-2724, CVE-2023-2935 a CVE-2023-2936 sú chyby zámeny typu premennej v komponente V8.

Zraniteľné systémy:

Google Chrome pre Linux a Mac verzie staršej ako 114.0.5735.90a Windows verzie staršej ako 114.0.5735.90/91.

Odporúčania:

Odporúčame aktualizáciu prehliadača Chrome pre Linux a Mac aspoň na verziu 114.0.5735.90a Windows aspoň na verziu 114.0.5735.90/91.

Zdroje:

https://chromereleases.googleblog.com/2023/05/
https://chromereleases.googleblog.com/2023/05/stable-channel-update-for-desktop_30.html
https://chromereleases.googleblog.com/2023/05/stable-channel-update-for-desktop_16.html

4. Adobe Acrobat a Reader

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

Zdroje:

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

5. Frameworky

Microsoft .NET Framework

V mesiaci máj spoločnosť Microsoft neopravila žiadnu kritickú ani vysoko závažnú zraniteľnosť vo frameworku .NET.

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

Oracle Java

Veľká sada opráv je plánovaná na 18. júla 2023.

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

6. Iné závažné zraniteľnosti

Cisco opravuje kritické zero-day zraniteľnosti prepínačov

Spoločnosť Cisco opravila viacero kritických a vysoko závažných zraniteľností vo svojom produktovom rade Small Business Series Switches. Zraniteľnosti sa týkajú nevhodnej validácie požiadaviek posielaných na používateľské sieťové rozhranie. Štyri kritické umožňujú vzdialené vykonávanie kódu a existuje pre verejne dostupný kód pre ich zneužitie. Ostatné umožňujú vyvolať nedostupnosť služby alebo dovoľujú čítať citlivé informácie. Viac informácií na stránke.

Apple rapídna bezpečnostná odpoveď na nové zero-day zraniteľnosti

Bezpečnostní výskumníci objavili tri zero-day zraniteľnosti zariadení spoločnosti Apple, ktoré útočníci používajú na sledovanie a zbieranie citlivých údajov zo zariadení iPhone, Mac a iPad. Spoločnosť Apple preto vydáva novú aktualizáciu zabezpečenia svojich zariadení formou nedávno spustenej služby rapídna bezpečnostná odpoveď (RSR). Viac informácií na stránke.

Zraniteľnosť v protokole SLP môže byť zneužitá na zosilnené DDoS útoky

Vysoko závažná zraniteľnosť v protokole SLP vyvoláva obavy z doteraz najväčšieho potencionálu zosilnenia pre reflektovaný útok s cieľom vyvolať nedostupnosť služby (DoS), aký kedy bol zaznamenaný. Viac informácií na stránke.

VMware opravuje kritické zreťaziteľné zero-day zraniteľnosti

Spoločnosť VMware opravuje dve zraniteľnosti nultého dňa, ktoré by mohli byť zreťazené a použité na spúšťanie kódu s neopravenými verziami firemných softvérových hypervízorov na

produktoch Workstation a Fusion. Zraniteľnosti boli odhalené na hackerskej súťaži Pwn20wn vo Vancouveri, Kanada. Viac informácií na stránke.

Kritické zraniteľnosti v zariadeniach UPS môžu spôsobiť nedostupnosť služby

UPS zariadenia spravované s APC Easy UPS Online Monitoring Softvér sú ohrozené chybami, ktoré môžu byť využité na vzdialené vykonávanie kódu, zmenu oprávnení alebo ich obídenie. V konečnom dôsledku hrozí strata funkčnosti nepretržitého napájania zariadení. Viac informácií na stránke.