Mesačný prehľad kritických zraniteľností
február 2023

1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci február 4 kritické a 32 vysoko závažných zraniteľností.

Všetky štyri kritické zraniteľnosti umožňujú vzdialené vykonávanie kódu. Zraniteľnosti CVE-2023-21689, CVE-2023-21690 a CVE-2023-21692 sa nachádzajú v Protected Extensible Authentication protokole (PEAP). Neautentifikovaný útočník môže zraniteľnosti zneužiť zaslaním špeciálne vytvoreného PEAP paketu zraniteľnému serveru, alebo sieťovým volaním. Kritická zraniteľnosť CVE-2023-21803 sa nachádza v službe Windows iSCSI Discovery. Útočník ju môže zneužiť zaslaním špeciálne vytvorenej požiadavky DHCP Discovery zraniteľnej službe iSCSI Discovery Service na 32 bitových zariadeniach.

Zraniteľnosti vysokej závažnosti umožňujú vzdialené vykonávanie kódu a eskaláciu oprávnení. Zneužitie niektorých z nich môže viesť k úniku informácií a vyvolaniu nedostupnosti služby.

Zraniteľné systémy:

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-2023-21689
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21690
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21692
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21803

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci február 1 kritickú a 8 vysoko závažných zraniteľností.

Kritická zraniteľnosť CVE-2023-21716 sa nachádza v Microsoft Word a umožňuje vzdialené vykonávanie kódu. Neautentifikovaný útočník môže zraniteľnosť zneužiť zaslaním škodlivého súboru RTF obeti. Tak získa možnosť vykonávať príkazy v aplikácii použitej na otvorenie dokumentu. Útok môže prebehnúť úspešne aj po samotnom zobrazení náhľadu škodlivého dokumentu (v Preview Pane).

Opravené vysoko závažné zraniteľnosti umožňujú vzdialené vykonávanie kódu, získanie vyšších oprávnení, možnosť obísť bezpečnostné prvky, či získavanie citlivých informácií.

Zraniteľné systémy:

3D Builder
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 for Android
Microsoft Office for iOS
Microsoft Office for Universal

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 Office Web Apps Server 2013 Service Pack 1
Microsoft OneNote for Android
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
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)
Print 3D
SharePoint Server Subscription Edition Language Pack

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-2023-21716

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft ukončila podporu prehliadača Internet Explorer 15.6.2022 pre hlavnú líniu operačných systémov Windows 10. Pre zvyšné operačné systémy, kde je prehliadač ešte podporovaný, nevydala v mesiaci február žiadne opravy kritických a závažných zraniteľností.

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

Microsoft Edge

Spoločnosť Microsoft v mesiaci február neopravila v prehliadači Microsoft Edge žiadnu kritickú ani vysoko závažnú zraniteľnosť.

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

Mozilla Firefox

V mesiaci február bolo opravených 11 vysoko závažných zraniteľností v línii Firefox a Firefox ESR.

Zraniteľnosť CVE-2023-25728 umožňuje získať URI z iframe-u potomka z hlavičky Content-Security-Policy-Report-Only, pokiaľ interakcia s daným iframe vyvolá presmerovanie.

Zraniteľnosť CVE-2023-25730 dovoľuje procesu na pozadí vyvolať requestFullscreen, čo môže viesť k nevyžiadanému prepnutiu prehliadača do režimu na celú obrazovku.

Zraniteľnosť CVE-2023-0767 umožňuje útočníkovi pomocou škodlivého certifikátu PKCS 12 zneužitím atribútov Safe Bag získať možnosť zápisu do pamäte.

Zraniteľnosť CVE-2023-25735 sa nachádza v nástroji SpiderMonkey a môže viesť k možnosti použitia dealokovanej pamäte.

Zraniteľnosť CVE-2023-25737 neplatné pretypovanie z nsTextNode do SVGElement môže viesť k nedefinovanému správaniu.

Zraniteľnosť CVE-2023-25738 spôsobuje na operačnom systéme Windows pád prehliadača pri pokuse tlačiť, kvôli nevhodnému narábaniu s niektorými ovládačmi.

Zraniteľnosť CVE-2023-25739 súvisí s absentujúcou kontrolou zrušenia zlyhaných požiadaviek na nahratie modulov. To môže viesť v komponente ScriptLoadContext k použitiu dealokovaného miesta v pamäti.

Zraniteľnosť CVE-2023-25743 postihuje iba rad Firefox Focus. Súvisí s absenciou oznámenia o prepnutí do režimu plnej obrazovky.

Označenia CVE-2023-25744 (Firefox a Firefox ESR), CVE-2023-25745 (Firefox) a CVE-2023-25746 (Firefox ESR) pokrývajú sadu zraniteľností ovplyvňujúcich bezpečnosť pamäte, ktoré môžu viesť ku poškodeniu pamäte alebo možnosti vykonávať kód.

Zraniteľné systémy:
Mozilla Firefox verzie staršie ako 110
Mozilla Firefox ESR verzie staršej ako 102.8

Odporúčania:
Odporúčame aktualizáciu Mozilla Firefox na verziu 110 a Mozilla Firefox ESR na verziu 102.8

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-05/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-06/

Google Chrome
V mesiaci február bola vydaná oprava 1 kritickej a 9 vysoko závažných zraniteľností prehliadača Google Chrome.

Kritická zraniteľnosť CVE-2023-0941 a vysoko závažné zraniteľnosti CVE-2023-0927, CVE-2023-0928, CVE-2023-0929, CVE-2023-0931 a CVE-2023-0932 0472 umožňujú použiť dealokované miesto v pamäti v komponentoch Prompts, Web Payments API, SwiftShader, Vulkan, Video a WebRTC.

CVE-2023-0930 súvisí s pretečením medzipamäte na halde v komponente Video.

Zraniteľnosť CVE-2023-0696 je chyba zámeny typu premennej v komponente V8.

CVE-2023-0697 súvisí s nevhodnou implementáciou režimu celej obraozvky.

CVE-2023-0698 v komponente WebRTC dovoľuje zapisovať mimo povolené hodnoty v pamäti.

Zraniteľné systémy:
Google Chrome pre Windows, Mac a Linux verzie staršej ako 110.0.5481.177.

Odporúčania:
Odporúčame aktualizáciu prehliadača Chrome pre Windows, Mac a Linux aspoň na verziu 110.0.5481.177/.178.

Zdroje:

https://chromereleases.googleblog.com/2023/02/
https://chromereleases.googleblog.com/2023/02/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2023/02/stable-channel-desktop-update_22.html

4. Adobe Acrobat a Reader

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

Zdroje:

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

5. Frameworky

Microsoft .NET Framework

V mesiaci február spoločnosť Microsoft opravila 1 kritickú a 1 vysoko závažnú zraniteľnosť vo frameworku .NET.

Kritická zraniteľnosť CVE-2023-21808 umožňuje vzdialené vykonávanie kódu. Zneužitie vysoko závažnej CVE-2023-21722 môže viesť k nedostupnosti služby.

Zraniteľné systémy:
.NET 6.0
.NET 7.0
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.0 Service Pack 2
Microsoft .NET Framework 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-2023-21808

Oracle Java

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

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

6. Iné závažné zraniteľnosti

Kritická zraniteľnosť ClamAV, Cisco Secure Endpoint a Secure Web Appliance umožňuje vykonávať kód

Spoločnosť Cisco vydala aktualizácie opravujúce kritickú zraniteľnosť v ClamAV, ktorá ovplyvňuje aj produkty Cisco Secure Endpoint, Secure Endpoint Private Cloud a Secure Web Appliance. Zraniteľnosť umožňuje vzdialené vykonávanie kódu s oprávneniami skeneru ClamAV. Viac informácií na stránke.

Microsoft opravil tri závažné zero-day zraniteľnosti

Spoločnosť Microsoft opravila tri vysoko závažné aktívne zneužívané zraniteľnosti vo viacerých svojich produktoch. Opravné aktualizácie boli vydané v rámci februárového balíka Patch Tuesday. Zraniteľnosti umožňujú vzdialene vykonávať kód, obchádzať blokovanie makier, či získať oprávnenia na úrovni SYSTEM. Viac informácií na stránke.

Kritická zraniteľnosť FortiNAC má exploit, FortiWeb možno onedlho

Spoločnosť Fortinet opravila 2 kritické zraniteľnosti vo svojich produktoch FortiNAC a FortiWeb, ktoré umožňujú vzdialene vykonávať kód. Pre jednu z nich bol publikovaný kód pre jej zneužitie. Spoločnosť odporúča bezodkladne aktualizovať zraniteľné zariadenia. Okrem toho tento mesiac opravila vo svojich produktoch ďalších 15 vysoko závažných zraniteľností. Viac informácií na stránke.