Mesačný prehľad kritických zraniteľností marec 2023

1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci marec 8 kritických a 47 vysoko závažných zraniteľností.

Kritická zraniteľnosť CVE-2023-1017 sa nachádza v knižnici modulu TPM2.0 a umožňuje získať vyššie oprávnenia. Útočník môže pomocou škodlivých príkazov TPM z hosťovského virtuálneho stroja dosiahnuť u obeti, ktorá používa Hyper-V, zápis mimo povolených hodnôt v kmeňovej partícii. Druhá zraniteľnosť v knižnici TPM2.0, CVE-2023-1018, umožňuje útočníkovi tiež zvýšiť svoje oprávnenia.

Zraniteľnosť CVE-2023-23411 sa nachádza v Hyper-V a jej zneužitie v hosťovskom systéme môže viesť k nedostupnosti hostiteľa (DoS).

Zvyšné opravené kritické zraniteľnosti umožňujú útočníkom vzdialene vykonávať kód. CVE-2023-21708 sa nachádza v protokole RPC a neautentifikovaný útočník ju môže zneužiť odoslaním špeciálne vytvoreného RPC volania RPC hostiteľovi. Tak môže vykonať kód na serveri s oprávneniami zneužitej RPC služby.

CVE-2023-23392 sa nachádza v protokole HTTP a neautentifikovanému útočníkovi dovoľuje vykonať kód odoslaním špeciálne vytvoreného paketu zraniteľnému serveru, s využitím ovládača http.sys.

CVE-2023-23404 sa nachádza v protokole PPTP a neautentifikovanému útočníkovi dovoľuje vykonať kód na serveri RAS odoslaním špeciálne vytvorenej požiadavky na pripojenie.

CVE-2023-23415 sa nachádza v protokole ICMP a útočník ju môže zneužiť odoslaním chybového hlásenia obsahujúceho fragmentovaný IP paket vložený v ICMP pakete.

CVE-2023-23416 sa nachádza v komponente Windows Cryptographic Services a zneužiť ju je možné importovaním škodlivého certifikátu v zraniteľnom systéme.

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-2023-1017
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1018
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21708
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23392
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23404
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23411
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23416

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci marec 1 kritickú a 10 vysoko závažných zraniteľností.

Kritická zraniteľnosť CVE-2023-23397 sa nachádza v Microsoft Outlook a umožňuje získať na diaľku zvýšené oprávnenia v zraniteľnom systéme bez interakcie obete. Útočník môže exfiltrovať Net-NTLMv2 haše a získať prístup k citlivým e-mailom. Zraniteľnosť je aktívne zneužívaná už takmer rok.

Opravené vysoko závažné zraniteľnosti umožňujú vzdialené vykonávanie kódu, získanie vyšších oprávnení, možnosť obísť bezpečnostné prvky, či získavanie citlivých informácií. Útočník ich môže zneužiť pri predstieraní cudzej identity a pre vyvolanie nedostupnosti služby.

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 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 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 for Android
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 Outlook 2013 RT Service Pack 1
Microsoft Outlook 2013 Service Pack 1 (32-bit editions)
Microsoft Outlook 2013 Service Pack 1 (64-bit editions)
Microsoft Outlook 2016 (32-bit edition)
Microsoft Outlook 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
OneDrive for Android
OneDrive for iOS
OneDrive for MacOS Installer

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-2023-23397

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 marec žiadne opravy kritických a závažných zraniteľností.

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

Microsoft Edge

Spoločnosť Microsoft v mesiaci marec opravila v prehliadači Microsoft Edge jednu vysoko závažnú zraniteľnosť.

Zraniteľnosť CVE-2023-24892 sa nachádza v komponente Webview2 a umožňuje útočníkom presmerovať obeť na škodlivú webstránku. K tomu potrebuje presvedčiť obeť, aby klikla na podvrhnutý odkaz.

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 marec bolo opravených 7 vysoko závažných zraniteľností v línii Firefox a Firefox ESR. Prvá štyri uvedené zraniteľnosti sa nachádzajú iba v línii Firefox.

CVE-2023-28159 umožňuje na Firefox pre Android ukryť oznámenie o prepnutí do režimu plnej obrazovky využitím vyskakovacích okien s informáciou o sťahovaní. Útočník by chybu mohol zneužiť na zmätenie obete.

CVE-2023-25748 umožňuje na Firefox pre Android ukryť oznámenie o prepnutí do režimu plnej obrazovky využitím vyskakovacieho okna s výzvou. Útočník by chybu mohol zneužiť na zmätenie obete.

CVE-2023-25749 umožňuje na Firefox pre Android otvoriť neaktualizované zraniteľné aplikácie pomocou komponentu Intents, bez predchádzajúceho zobrazenia upozornenia.

CVE-2023-25750 spôsobuje za nešpecifikovaných okolností únik offline obsahu vyrovnávacej pamäte komponentu ServiceWorker do súborového systému počas prehliadania v súkromnom režime.

CVE-2023-25751 v prehliadači Firefox a Firefox ESR súvisí s nesprávnym prepisom novo generovaného JIT kódu pri iterovaní.

Označenia CVE-2023-28176 (Firefox a Firefox ESR) a CVE-2023-28177 (Firefox) pokrývajú sadu zraniteľností ovplyvňujúcich bezpečnosť pamäte, ktoré môžu viesť ku poškodeniu pamäte alebo možnosti vykonávať kód.

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 111
Mozilla Firefox ESR verzie staršej ako 102.9

Odporúčania:
Odporúčame aktualizáciu Mozilla Firefox na verziu 111 a Mozilla Firefox ESR na verziu 102.9

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-09/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-10/

Google Chrome
V mesiaci marec bola vydaná oprava 15 vysoko závažných zraniteľností prehliadača Google Chrome.

Zraniteľnosti CVE-2023-1213, CVE-2023-1216, CVE-2023-1218, CVE-2023-1528, CVE-2023-1530, CVE-2023-1531 a CVE-2023-1533 umožňujú použiť dealokované miesto v pamäti v komponentoch Swiftshader, DevTools, WebRTC, Passwords, PDF, ANGLE a WebProtect.

Zraniteľnosti CVE-2023-1214 a CVE-2023-1215 sú chyby zámeny typu premennej v komponentoch V8 a CSS.

CVE-2023-1217 súvisí s pretečením medzipamäte zásobníka v komponente pre reportovanie zlyhaní (Crash).

CVE-2023-1219 a CVE-2023-1220 súvisia s pretečením medzipamäte na halde v komponente Metrics a UMA.

Zraniteľnosti CVE-2023-1529, CVE-2023-1532 a CVE-2023-1534 v komponentoch WebHID, GPU Video a ANGLE dovoľujú čítať mimo povolené hodnoty v pamäti.

Zraniteľné systémy:
Google Chrome pre Windows, Mac a Linux verzie staršej ako 111.0.5563.110.

Odporúčania:
Odporúčame aktualizáciu prehliadača Chrome pre Windows, Mac a Linux aspoň na verziu 111.0.5563.110/.111.

Zdroje:

https://chromereleases.googleblog.com/2023/03/
https://chromereleases.googleblog.com/2023/03/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html

4. Adobe Acrobat a Reader

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

Zdroje:

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

5. Frameworky

Microsoft .NET Framework

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

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

Oracle Java

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

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

6. Iné závažné zraniteľnosti

Kritické zraniteľnosti SAP umožňujú vykonávať kód aj získať citlivé údaje

Spoločnosť SAP v marci opravila vo svojich produktoch 19 zraniteľností, z ktorých 5 je kritických. Útočníkom umožňujú vzdialene vykonávať príkazy, zasahovať do systémových súborov, získavať citlivé informácie a spôsobiť nedostupnosť služieb. Viac informácií na stránke.

Zero-day zraniteľnosť v Microsoft Outlook zneužívajú ruskí hackeri

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.

Kritická zraniteľnosť vo FortiOS a FortiProxy

Nová kritická chyba v produktoch FortiOS a FortiProxy poskytuje útočníkom vzdialený prístup, hrozí poškodenie pamäte. Chyba bola označená CVSS ako závažná v stupnici 9,3 z 10. Kód chyby CVE-2023-25610. Viac informácií na stránke.

WiFi – chyba v protokole umožňuje získať obsah rámcov

Bezpečnostní výskumníci z Northeastern University a KU Leuven objavili zraniteľnosť v mechanizme štandardu WiFi 802.11b pre narábanie so sieťovými rámcami určenými pre uspaté zariadenia. Útočníkom umožňuje získavať obsah rámcov určených pre ľubovoľné zariadenie v sieti, či posielať rámce so škodlivým obsahom. Zraniteľnosť sa týka širokej škály WiFi prístupových bodov a operačných systémov. Viac informácií na stránke.