Mesačný prehľad kritických zraniteľností marec 2022

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci marec 2 kritické a 41 závažných zraniteľností súvisiacich s operačným systémom Windows.

Kritická zraniteľnosť CVE-2022-22006 sa vyskytuje v rozšíreniach HEVC Video a druhá kritická zraniteľnosť CVE-2022-24501 sa nachádza v rozšíreniach VP9 Video. Obe zraniteľnosti môžu viesť k vzdialenému vykonaniu kódu. Útočník môže zraniteľnosti zneužiť nalákaním obete, aby si stiahla a otvorila špeciálne vytvorený súbor, ktorý môže viesť k zlyhaniu systému.

Deväťnásť zo závažných zraniteľností môže viesť k eskalácii privilégií. Ďalších 13 zraniteľností súvisí so vzdialeným vykonaním kódu. Zneužitím iných 5 zraniteľností môže dôjsť k úniku citlivých informácií. Tri závažné zraniteľnosti môžu spôsobiť narušenie dostupnosti služby. Posledná zraniteľnosť môže umožniť obídenie bezpečnostných prvkov.

Zraniteľné systémy:

HEIF Image Extension
HEVC Video Extensions
Raw Image Extension
Remote Desktop client for Windows Desktop
VP9 Video Extensions
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 1909 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 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 21H1 for 32-bit Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows 10 Version 21H1 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 11 for ARM64-based Systems

Windows 11 for x64-based Systems
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
Windows RT 8.1
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)
Windows Server 2022 Azure Edition Core Hotpatch
Windows Server, version 20H2 (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://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-22006
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-24501

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci marec 8 závažných zraniteľností. Štyri zo závažných zraniteľností (CVE-2022-23282, CVE-2022-24461, CVE-2022-24509 a CVE-2022-24510) umožňujú útočníkom vzdialené vykonávanie kódu. Zraniteľnosť CVE-2022-24522 môže viesť k odhaleniu citlivých informácií. Zneužitím zraniteľnosti CVE-2022-24511 môže dôjsť k falšovaniu údajov. Zraniteľnosť CVE-2022-21987 môže umožniť predstieranie cudzej identity. Posledné dve zraniteľnosti (CVE-2022-24462 a CVE-2022-24465) môžu umožniť obídenie bezpečnostných prvkov.

Zraniteľné systémy:

Intune Company Portal for iOS
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 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 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)
Paint 3D
Skype Extension for Chrome

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 neopravila tento mesiac v prehliadači Internet Explorer žiadnu kritickú ani závažnú zraniteľnosť.

Zdroje:

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

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac v prehliadači Edge jednu závažnú zraniteľnosť (CVE-2022-26899), ktorá môže viesť k eskalácii privilégií.

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

Mozilla Firefox

V mesiaci marec boli v prehliadači Firefox a Firefox ESR opravené 2 kritické a 4 závažné zraniteľnosti.

Kritická zraniteľnosť CVE-2022-26485 súvisí s vymazaním parametra XSLT pri spracovávaní XML dokumentu. To umožňuje útočníkovi využiť dealokované miesto v pamäti, pomocou čoho môže vykonať vlastný škodlivý kód. Druhá kritická zraniteľnosť CVE-2022-26486 súvisí s chybou platformy WebGPU IPC, kde môže útočník zneužitím dealokovaného miesta v pamäti opustiť sandbox prehliadača, a tak vykonávať škodlivý kód v rámci systému.

CVE-2022-26383 – pri zmene veľkosti okna na režim celej obrazovky sa v kontextovom okne nezobrazí upozornenie na celú obrazovku.

CVE-2022-26384 – ak by útočník mohol kontrolovať obsah prvku iframe v sandboxe s povolenými vyskakovacími oknami, ale nie s povolenými skriptami, dokázal by vytvoriť odkaz, ktorý by po kliknutí viedol k spusteniu JavaScriptu.

CVE-2022-26387 súvisí s doplnkami. Pri inštalácii Firefox overil podpis pred vyzvaním používateľa. Kým používateľ potvrdzoval výzvu, základný súbor doplnku mohol byť modifikovaný.

CVE-2022-26381 sa týka použitia odalokovaného miesta v pamäti. Jedná sa o vynútenie preformátovania textu v objekte SVG, čo môže viesť k zneužitiu.

Zraniteľné systémy:
Mozilla Firefox verzie staršej ako 98
Mozilla Firefox ESR verzie staršej ako 91.7

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 98 a Firefox ESR na verziu 91.7.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-09/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-10/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-11/

Google Chrome

V mesiaci marec bola vydaná oprava pre 1 kritickú a 28 závažných zraniteľností. Kritická zraniteľnosť (CVE-2022-0971) sa vyskytuje v Blink Layout a súvisí s použitím odalokovaného miesta v pamäti.

Závažné zraniteľnosti sa väčšinou týkajú pretečenia medzipamäte haldy, čítania mimo povolených hodnôt, nesprávnej implementácie a použitia odalokovaného miesta v pamäti. Zraniteľnosti sa nachádzajú v komponentoch ako Portals, QR Code Generator, Full Screen Mode, Cast UI, ANGLE, V8, Mojo a ďalších.

Zraniteľné systémy:
Google Chrome pre Windows, Mac a Linux verzie staršej ako 99.0.4844.84

Odporúčania:
Odporúčame aktualizáciu prehliadača Chrome pre Windows, Mac a Linux na verziu 99.0.4844.84.

Zdroje:
https://chromereleases.googleblog.com/2022
https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_15.html
https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_20.html
https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_25.html
https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_29.html

4. Adobe Acrobat a Reader

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

Zdroje:
https://helpx.adobe.com/security.html

5. Frameworky

Microsoft .NET Framework

V mesiaci marec spoločnosť Microsoft opravila 3 závažné zraniteľnosti vo frameworku .NET. Zneužitím môže dôjsť k narušeniu dostupnosti služby alebo vzdialenému vykonaniu kódu.

Zraniteľné systémy:
.NET 5.0
.NET 6.0
.NET Core 3.1

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

Oracle Java

Veľká sada opráv je plánovaná na 19. apríl 2022.

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

6. Iné závažné zraniteľnosti

Zero-day zraniteľnosti produktov Mozilla

Spoločnosť Mozilla opravila dve zero-day zraniteľnosti, ktoré sa týkali vybraných produktov. Zraniteľnosti sú vysokej závažnosti s CVSS skóre 8.4. Viac informácií na stránke.

Kritické zraniteľnosti produktov Veeam

Spoločnosť Veeam vydala aktualizácie svojich produktov Veeam Backup & Replication, ktoré opravujú štyri novoobjavené zraniteľnosti. Tieto zraniteľnosti by mohli byť zneužité na kompromitáciu podnikovej infraštruktúry. Opravy boli vydané pre verzie Veeam Backup & Replication 10 a 11. Spoločnosť Veeam odporúča používateľom starších verzií produktov migráciu na podporované verzie. Viac informácií na stránke.

Kritické zraniteľnosti tlačiarní HP umožňujú vzdialene vykonávať kód

Spoločnosť Hewlett Packard vydala opravné aktualizácie pre stovky modelov tlačiarní a multifunkčných zariadení, v ktorých bolo objavených niekoľko kritických zraniteľností. Tieto chyby umožňujú vzdialené vykonávanie kódu, spôsobenie nedostupnosti systému a únik informácií. Viac informácií na stránke.

Zraniteľnosť služby Redis

V službe Redis pre distribúcie Linux rodiny Debian bola nájdená kritická zraniteľnosť s CVSSv3 skóre 10. Zraniteľnosť umožňuje vzdialene vykonávať kód a zneužíva ju botnet Muhstik. Viac informácií na stránke.