Mesačný prehľad kritických zraniteľností
Júl 2022

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci júl 4 kritické zraniteľnosti a 80 vysoko závažných zraniteľností súvisiacich s operačným systémom Windows.

Opravené kritické zraniteľnosti umožňujú vzdialené vykonávanie kódu. Nachádzajú sa v komponentoch Windows Network File System (CVE-2022-22029, CVE-2022-22039), Remote Procedure Call Runtime (CVE-2022-22038) a Windows Graphics Component (CVE-2022-30221).

Zraniteľnosti vysokej závažnosti umožňujú eskaláciu oprávnení, únik dát, obídenie bezpečnostných prvkov, vzdialené vykonávanie kódu, spôsobiť nedostupnosť služby, či neoprávnene nahrávať potenciálne škodlivé súbory.

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 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30221
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22029
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22038
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22039

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci júl 2 závažné zraniteľnosti.

Opravená bola zraniteľnosť CVE-2022-33632, ktorá umožňuje obídenie bezpečnostných prvkov pre chybu autorizácie. Druhá zraniteľnosť CVE-2022-33633 sa nachádza v Skype for Business a Lync a umožňuje vzdialene vykonávať kód.

Zraniteľné systémy:

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Office 2016 (32-bit edition)
Microsoft Office 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 Lync Server 2013 CU10
Skype for Business Server 2015 CU12
Skype for Business Server 2019 CU6
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions

Microsoft Office LTSC 2021 for 64-bit editions

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-2022-33632
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-33633

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 júl žiadne opravy kritických a závažných zraniteľností.

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

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac 7 závažných zraniteľností v prehliadači Edge založenom na platforme Chromium.

Spoločnosť Google vydala pre Chromium aktualizácie zabezpečenia zraniteľností umožňujúcich použitie dealokovaného miesta v pamäti (CVE-2022-2478, CVE-2022-2477 a CVE-2022-2480, CVE-2022-2481), vedúcich k poškodeniu haldy (CVE-2022-2295), pretečeniu haldy (CVE-2022-2294) a súvisiacich s nedostatočným overením nedôveryhodného vstupu (CVE-2022-2479).

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-2022-2477
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2478
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2479
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2480
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2481
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2295
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2294

Mozilla Firefox
V mesiaci júl boli v prehliadači Firefox a Firefox ESR opravené 2 závažné zraniteľnosti.

Závažné zraniteľnosti CVE-2022-2505 a CVE-2022-36320 umožňujú vykonanie ľubovoľného kódu pre možné poškodenie pamäte.

Zraniteľné systémy:
Mozilla Firefox verzie 103 a 102

Odporúčania:
Odporúčame aktualizáciu na verziu 103.0.1 a 102.1.0

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-28/#CVE-2022-2505
https://www.mozilla.org/en-US/security/advisories/mfsa2022-28/#CVE-2022-36320

Google Chrome
V mesiaci júl bola vydaná oprava na 27 zraniteľností, z toho 7 závažných.

Závažné zraniteľnosti ako CVE-2022-2603, CVE-2022-2604, CVE-2022-2605, CVE-2022-2606, CVE-2022-2607, CVE-2022-2608 a CVE-2022-2609 umožňujú použitie dealokovaného miesta v pamäti. Nachádzajú sa v komponentoch Omnibox, Safe Browsing, Managed devices API, Tab Strip, Overview Mode či Nearby Share.

Zraniteľnosť CVE-2022-2605 v komponente Dawn dovoľuje čítanie pamäte mimo povolených hodnôt.

Zraniteľné systémy:
Google Chrome verzie staršie ako 104.0.5112.79/80/81 (Windows)
104.0.5112.79 (Mac/Linux)

Odporúčania:
Odporúčame aktualizáciu na verziu 104.0.5112.79/80/81 (Windows) / 104.0.5112.79 (Mac/Linux)

Zdroje:

https://chromereleases.googleblog.com/2019
https://chromereleases.googleblog.com/2019/07/stable-channel-update-for-desktop.html

4. Adobe Acrobat a Reader

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

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

5. Frameworky

Microsoft .NET Framework

V mesiaci júl nebola spoločnosťou Microsoft opravená žiadna zraniteľnosť frameworku .NET.

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

Oracle Java

Spoločnosť Oracle vydala v mesiaci júl opravy 5 zraniteľností v rámci Oracle Java SE. Najzávažnejšia zraniteľnosť má skóre CVSSv3.1 - 7,5.

Zraniteľnosti a zraniteľné systémy:

CVE-2022-34169 (CVSS 7.5) Oracle Java SE: 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1; Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2, 22.1.0
CVE-2022-25647 (CVSS 6.2) Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2, 22.1.0
CVE-2022-21541 (CVSS 5.9) Oracle Java SE: 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1; Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2, 22.1.0
CVE-2022-21540 (CVSS 5.3) Oracle Java SE: 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1; Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2, 22.1.0
CVE-2022-21549 (CVSS 5.3)
Oracle Java SE: 17.0.3.1; Oracle GraalVM Enterprise Edition: 21.3.2, 22.1.0

Odporúčania:

Odporúčame aktualizovať zraniteľné verzie Java SE na aktuálne verzie prostredníctvom Java Auto Update alebo na stránke spoločnosti Oracle, viď prvý odkaz v zdrojoch.

Zdroje:

https://www.oracle.com/security-alerts/cpujul2022.html

6. Iné závažné zraniteľnosti

Kritické zraniteľnosti produktov Atlassian

Spoločnosť Atlassian vydala opravy pre 3 kritické zraniteľnosti vo svojich produktoch Bamboo, Bitbucket, Confluence, Crowd, Fisheye, Crucible a Jira. Útočník môže po ich úspešnom zneužití vzdialene vykonať JavaScript kód, či získať prístup do zraniteľnej platformy s právami obete. Viac informácií na stránke.