Mesačný prehľad kritických zraniteľností júl 2021

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci júl 8 kritických a 83 závažných zraniteľností. Všetky kritické zraniteľnosti môžu viesť k vzdialenému vykonaniu kódu.

Kritická zraniteľnosť CVE-2021-33740 sa vyskytuje vo Windows Media. Súvisí s nesprávnym overením vstupu, pričom úspešným zneužitím môže dôjsť k úplnej kompromitácii zraniteľného systému.

Ďalšie kritické zraniteľnosti sú CVE-2021-34439 a CVE-2021-34503. Nachádzajú sa v Microsoft Windows Media Foundation. Obe zraniteľnosti existujú z dôvodu nesprávneho overenia vstupu. Vzdialený útočník môže odoslať špeciálne vytvorenú požiadavku a vykonať ľubovoľný kód v cieľovom systéme.

Zraniteľnosť CVE-2021-34448 sa nachádza v skriptovacom nástroji a súvisí s poškodením pamäte. Táto chyba existuje kvôli hraničnej chybe pri spracovávaní HTML obsahu. Útočník vytvorí špeciálnu webovú stránku a naláka používateľa, aby ju otvoril. Následne môže dôjsť k poškodeniu pamäte, čo môže viesť k vzdialenému vykonaniu kódu. Zraniteľnosť je aktívne zneužívaná útočníkmi.

Ďalšia zraniteľnosť sa nachádza vo Windows Hyper-V a jej označenie je CVE-2021-34450. Takisto existuje z dôvodu nesprávneho overenia vstupu. Úspešným zneužitím by mohlo dôjsť k úplnej kompromitácii systému.

Zraniteľnosť CVE-2021-34458 sa nachádza vo Windows Kerneli. Chyba umožňuje SR-IOV zariadeniu, ktoré je priradené hosťovi, potenciálne narušiť PCIe, ktoré sú pripojené k iným hosťom alebo k root-ovi.

CVE-2021-34494 sa nachádza vo Windows DNS Serveri. Chyba súvisí s nesprávnym overovaním vstupu. Úspešným zneužitím je útočník schopný kompromitovať zraniteľný systém.

Posledná kritická zraniteľnosť je CVE-2021-34497. Nachádza sa v platforme Microsoft MSHTML. Zneužitie vyžaduje interakciu používateľa – útočník musí nalákať používateľa na špeciálne zdieľané umiestnenie na serveri alebo na navštívenie škodlivej webovej stránky.

Zraniteľné systémy:
HEVC 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 2004 for 32-bit Systems
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 2004 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 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, version 1909 (Server Core installation)
Windows Server, version 2004 (Server Core installation)
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-2021-33740
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-34439
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-34448
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-34450
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-34458
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-34494
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-34497

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-34503

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci júl 10 závažných zraniteľností. Šesť zo závažných zraniteľností (CVE-2021-34452, CVE-2021-34467, CVE-2021-34468, CVE-2021-34501, CVE-2021-34518 a CVE-2021-34520) umožňuje útočníkom vzdialené vykonávanie kódu. Zneužitím zraniteľností CVE-2021-33753, CVE-2021-34451 a CVE-2021-34517 môže dôjsť k umožneniu predstierania cudzej identity. Zraniteľnosť CVE-2021-34469 môže viesť k obídeniu bezpečnostných prvkov.

Zraniteľné systémy:

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Bing Search for Android
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 Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1
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 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://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 Microsoft Edge 3 závažné zraniteľnosti. Zraniteľnosti CVE-2021-36928 a CVE-2021-36931 môžu viesť k eskalácii privilégií a zneužitím CVE-2021-36929 môže dôjsť k úniku informácií.

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 júl nebola v prehliadači Firefox a Firefox ESR opravená žiadna kritická zraniteľnosť. V prehliadači Firefox bolo opravených 5 závažných zraniteľností, pričom 3 z nich sa vyskytujú aj v prehliadači Firefox ESR.

Závažná zraniteľnosť CVE-2021-29970 vyskytujúca sa v oboch prehliadačoch môže viesť k poškodeniu pamäte a použitiu odalokovaného miesta v pamäti. Chyba ovplyvňuje prehliadače, ktoré majú povolené funkcie „Accessibility“.

Ďalšia zraniteľnosť oboch prehliadačov CVE-2021-30547 sa vyskytuje v knižnici ANGLE a súvisí so zápisom mimo povolených hodnôt. Zneužitím môže dôjsť k poškodeniu pamäte.

Posledné bezpečnostné chyby CVE-2021-29976 v oboch prehliadačoch Firefox a Firefox ESR boli označené ako chyby pamäte. Niektoré môžu viesť k poškodeniu pamäte a s dostatočným úsilím by útočník mohol vzdialene vykonať kód. Chyby s rovnakým dopadom sa v prehliadači Firefox vyskytujú aj pod označením CVE-2021-29977.

V prehliadači Firefox pre Android sa vyskytuje zraniteľnosť CVE-2021-29971. Ak by používateľ udelil povolenie webovej stránke a uložil ho, takéto povolenie by sa udelilo akejkoľvek stránke bežiacej na tom istom zariadení.

Zraniteľné systémy:
Mozilla Firefox pre Android verzie staršej ako 90
Mozilla Firefox ESR verzie staršej ako 78.12.

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 90 a Firefox ESR na verziu 78.12.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-28/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-29/

Google Chrome

V mesiaci júl bola vydaná oprava pre 15 závažných zraniteľností. Zraniteľnosti sa väčšinou týkajú použitia odalokovaného miesta v pamäti, pretečenia medzipamäte haldy alebo zásobníka a zápisu mimo povolených hodnôt. Zraniteľnosti sa nachádzajú v komponentoch ako Autofill, WebGL, TabGroups, sqlite a ďalších.

Zraniteľné systémy:
Google Chrome verzie staršej ako 92.0.4515.107

Odporúčania:
Odporúčame aktualizáciu na verziu 92.0.4515.107

Zdroje:
https://chromereleases.googleblog.com/2021
https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop.html

https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html

4. Adobe Flash Player, Acrobat a Reader

V produkte Adobe Acrobat a Reader bolo v júli opravených 13 kritických zraniteľností.

Kritické zraniteľnosti CVE-2021-28640, CVE-2021-28641, CVE-2021-28639, CVE-2021-35983, CVE-2021-35981 a CVE-2021-28635 súvisia s použitím odalokovaného miesta v pamäti. Zneužitím sú útočníci schopní vzdialene vykonávať ľubovoľný kód.

CVE-2021-35980 a CVE-2021-28644 súvisia s prechádzaním ciest (Path Traversal). Zraniteľnosť CVE-2021-28643 existuje z dôvodu hraničnej podmienky pri spracovávaní PDF súborov. Úspešným zneužitím môže dôjsť k vykonaniu ľubovoľného kódu. CVE-2021-28642 súvisí so zápisom mimo povolených hodnôt. CVE-2021-28638 súvisí s pretečením medzipamäte haldy a môže viesť k vzdialenému vykonaniu kódu. Zraniteľnosť CVE-2021-28636 existuje z dôvodu, že aplikácia nenačítava DLL knižnice bezpečným spôsobom. CVE-2021-28634 súvisí s injektovaním príkazov. Lokálny používateľ môže vykonávať príkazy v rámci operačného systému a následne eskalovať privilégiá.

Adobe prestal vydávať záplaty pre Flash Player 31. decembra 2020, teda nie je bezpečné ho používať.

Zraniteľné systémy:
Acrobat DC
Acrobat Reader DC
Acrobat 2020
Acrobat Reader 2020
Acrobat 2017
Acrobat Reader 2017

Odporúčania:
Odporúčame aktualizáciu:
Acrobat DC na verziu 2021.005.20058
Acrobat Reader DC na verziu 2021.005.20058
Acrobat 2020 na verziu 2020.004.30006
Acrobat Reader 2020 na verziu 2020.004.30006
Acrobat 2017 na verziu 2017.011.30199
Acrobat Reader 2017 na verziu 2017.011.30199

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/acrobat/apsb21-51.html

5. Frameworky

Microsoft .NET Framework

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

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

Oracle Java

Spoločnosť Oracle vydala v mesiac júl plánovanú štvrťročnú veľkú sadu aktualizácií. V Oracle Java SE bolo dokopy opravených 6 zraniteľností, z čoho 1 je kritická a 1 je závažná. Kritická zraniteľnosť CVE-2021-29921 sa vyskytuje v komponente „Python interpreter and runtime (CPython)“. Zneužitím môže dôjsť k úniku citlivých informácií, modifikácií dát alebo k narušeniu dostupnosti služby.

Závažná zraniteľnosť CVE-2021-2388 sa vyskytuje v komponente „Hotspot“. Zneužitím môže dôjsť ku kompromitácii Java SE alebo Oracle GraalVM Enterprise Edition. Úspešný útok vyžaduje interakciu používateľa.

Zraniteľné systémy:
Oracle GraalVM Enterprise Edition: 20.3.2, 21.1.0
Java SE: 7u301, 8u291, 11.0.11, 16.0.1

Odporúčania:
Odporúčame aktualizovať zraniteľné verzie Oracle GraalVM Enterprise Edition a 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/
https://www.oracle.com/security-alerts/cpujul2021.html

6. Iné závažné zraniteľnosti

Kritická zraniteľnosť služby Print Spooler vo všetkých verziách Windows

V operačných systémoch Windows bola nájdená zraniteľnosť služby, ktorá sa využíva na komunikáciu s lokálnymi a sieťovými tlačiarňami. Spoločnosť Microsoft vydala opravnú aktualizáciu všetkých podporovaných systémov, avšak zraniteľnosť nebola odstránená. Pre zabezpečenie infraštruktúry odporúčame administrátorom vypnúť službu Print Spooler ak je to možné, alebo postupovať podľa odporúčaní Microsoft. Viac informácií na stránke.