Mesačný prehľad kritických zraniteľností september 2021

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci september 2 kritické a 32 závažných zraniteľností.

Kritická zraniteľnosť CVE-2021-26435 sa nachádza v skriptovacom nástroji. Existuje z dôvodu hraničnej chyby a môže viesť k vykonaniu ľubovoľného kódu na cieľovom systéme. Vzdialený útočník vytvorí špeciálny súbor, naláka obeť na otvorenie tohto súboru a následne môže spôsobiť poškodenie pamäte. Úspešným zneužitím môže dôjsť k úplnej kompromitácii zraniteľného systému.

Druhá kritická zraniteľnosť je CVE-2021-36965. Nachádza sa v službe WLAN AutoConfig. Existuje z dôvodu nesprávneho overenia vstupu. Vzdialený útočník v lokálnej sieti môže odoslať špeciálne vytvorenú požiadavku a vykonať ľubovoľný kód v cieľovom systéme.

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 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-2021-26435
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-36965

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci september 12 závažných zraniteľností. Deväť zo závažných zraniteľností (CVE-2021-38646 a CVE-2021-38653 až CVE-2021-38660) umožňuje útočníkom vzdialené vykonávanie kódu. Zneužitím zraniteľností CVE-2021-38650, CVE-2021-38651 a CVE-2021-38652 môže útočník získať schopnosť predstierať cudziu identitu.

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 Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1

Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2019

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 5 závažných zraniteľností. Zneužitím týchto zraniteľností môže dôjsť k manipulácii, falšovaniu identity alebo eskalácii privilégií.

Zdroje:

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

Mozilla Firefox

V mesiaci september nebola v prehliadači Firefox a Firefox ESR opravená žiadna kritická zraniteľnosť. V prehliadači Firefox boli opravené 4 závažné zraniteľnosti, pričom 2 z nich sa vyskytujú aj v prehliadači Firefox ESR.

CVE-2021-38493 sú chyby súvisiace s pamäťou v prehliadači Firefox 91 a Firefox ESR 78.14. S dostatočným úsilím by mohol útočník vzdialene vykonať kód. Chyby s označením CVE-2021-38495 taktiež súvisia s pamäťou. Niektoré z týchto chýb spôsobujú poškodenie pamäte a tiež by mohli byť zneužité na vykonanie ľubovoľného kódu.

V prehliadači Firefox pre Android sa vyskytuje zraniteľnosť CVE-2021-29993. Prehliadač umožňoval navigáciu prostredníctvom protokolu *intent://*, ktorý by mohol byť použitý na spôsobovanie zlyhaní a podvrhnutie falošného používateľského rozhrania.
CVE-2021-38494 sú chyby pamäte v prehliadači Firefox verzie 91. S dostatočným úsilím by mohol útočník vzdialene vykonať kód.

Zraniteľné systémy:
Mozilla Firefox pre Android verzie staršej ako 92
Mozilla Firefox ESR verzie staršej ako 91.1

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 92 a Firefox ESR na verziu 91.1.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-38/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-39/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-40/

Google Chrome

V mesiaci september bola vydaná oprava pre 15 závažných zraniteľností. Zraniteľnosti sa väčšinou týkajú použitia odalokovaného miesta v pamäti, nesprávnej implementácie, pretečenia medzipamäte zásobníka a zápisu mimo povolených hodnôt. Zraniteľnosti sa nachádzajú v komponentoch ako Selection API, ANGLE, V8, Blink a ďalších.

Zraniteľné systémy:
Google Chrome verzie staršej ako 94.0.4606.61

Odporúčania:
Odporúčame aktualizáciu na verziu 94.0.4606.61

Zdroje:
https://chromereleases.googleblog.com/2021
https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html

https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_24.html

4. Adobe Acrobat a Reader

V produkte Adobe Acrobat a Reader bolo v mesiaci september opravených 13 kritických a 9 závažných zraniteľností.

Kritické zraniteľnosti CVE-2021-39836, CVE-2021-39837, CVE-2021-39838, CVE-2021-39839, CVE-2021-39840 a CVE-2021-39842 súvisia s použitím odalokovaného miesta v pamäti. Ich zneužitím sú útočníci schopní vzdialene vykonávať ľubovoľný kód.

Zraniteľnosť CVE-2021-39852 sa týka dereferencie nulového ukazovateľa a jej zneužitím môže dôjsť k narušeniu dostupnosti služby.

CVE-2021-39845 a CVE-2021-39846 súvisia s pretečením medzipamäte zásobníka a CVE-2021-39863 s pretečením medzipamäte haldy. Zneužitím môže dôjsť k vykonaniu ľubovoľného kódu.

Ďalšie zraniteľnosti CVE-2021-39843 a CVE-2021-39844 súvisia s čítaním alebo zápisom mimo povolených hodnôt. Úspešným zneužitím by mohlo dôjsť k úniku pamäte.

Posledná kritická zraniteľnosť CVE-2021-39841 sa vyskytuje pri spracovávaní PDF súborov. Útočník môže nalákať obeť na otvorenie špeciálne vytvoreného súboru, následne vyvolať chybu typovej zámeny a vykonať ľubovoľný kód v cieľovom systéme.

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

Odporúčania:
Odporúčame aktualizáciu:
Acrobat DC na verziu 2021.007.20091
Acrobat Reader DC na verziu 2021.007.20091
Acrobat 2020 na verziu 2020.004.30015
Acrobat Reader 2020 na verziu 2020.004.30015
Acrobat 2017 na verziu 2017.011.30202
Acrobat Reader 2017 na verziu 2017.011.30202

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/acrobat/apsb21-55.html

5. Frameworky

Microsoft .NET Framework

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

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

Oracle Java

Veľká sada opráv je plánovaná na 19. október 2021.

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