Mesačný prehľad kritických zraniteľností
august 2021

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci august 7 kritických a 22 závažných zraniteľností. Všetky kritické zraniteľnosti môžu viesť k vzdialenému vykonaniu kódu.

Kritická zraniteľnosť CVE-2021-26424 sa vyskytuje vo Windows Hyper-V. Existuje z dôvodu hraničnej chyby v tcpip.sys pri spracovávaní TCP/IP paketov odosielaných pomocou protokolu IPv6. Vzdialený Hyper-V hosť môže poslať špeciálne vytvorenú IPv6 požiadavku na zraniteľného Hyper-V hostiteľa a spôsobiť tým poškodenie pamäte.

Ďalšia kritická zraniteľnosť má označenie CVE-2021-26432. Nachádza sa v Microsoft službách pre ovládač NFS ONCRPC XDR. Existuje z dôvodu nesprávneho overenia vstupu. Vzdialený útočník môže odoslať špeciálne vytvorenú požiadavku a vykonať ľubovoľný kód v cieľovom systéme.

Zraniteľnosť CVE-2021-34480 sa nachádza v skriptovacom nástroji. 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.

Ďalšia zraniteľnosť sa nachádza v komponente Windows Graphics. Jej označenie je CVE-2021-34530. Takisto existuje z dôvodu nesprávneho overenia vstupu. Úspešným zneužitím by mohlo dôjsť k úplnej kompromitácii systému.

Zraniteľnosť CVE-2021-34534 sa nachádza v platforme Microsoft MSHTML. Zneužitie vyžaduje interakciu používateľa – útočník musí nalákať používateľa, aby otvoril škodlivý súbor alebo na navštívil webovú stránku obsahujúcu špeciálne vytvorený súbor.

CVE-2021-34535 sa nachádza v klientovi vzdialenej plochy (Remote Desktop Client). Chyba súvisí s nesprávnym overovaním vstupu v klientovi vzdialenej plochy a v prehliadači Hyper-V (Hyper-V Viewer). Úspešným zneužitím je útočník schopný kompromitovať zraniteľný systém.

Posledná kritická zraniteľnosť je CVE-2021-36936. Nachádza sa v službe Print Spooler. Existuje z dôvodu nesprávneho overenia vstupu v službe. Vzdialený autentifikovaný útočník by mohol poslať špeciálne vytvorenú požiadavku a vykonať ľubovoľný kód v cieľovom systéme.

Zraniteľné systémy:

Remote Desktop client for Windows Desktop
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)
Windows Update Assistant

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-2021-26424
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-26432
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-34480
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-34530

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-34534
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-34535
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-36936

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci august 3 závažné zraniteľnosti. Dve zo závažných zraniteľností (CVE-2021-34478 a CVE-2021-36941) umožňujú útočníkom vzdialené vykonávanie kódu. Zneužitím zraniteľnosti CVE-2021-36940 v produktoch Microsoft SharePoint môže útočník získať možnosť úspešne predstierať cudziu identitu.

Zraniteľné systémy:
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 Mac
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
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 neopravila tento mesiac v prehliadači Edge žiadnu kritickú ani závažnú zraniteľnosť.

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

Mozilla Firefox

V mesiaci august nebola v prehliadači Firefox a Firefox ESR opravená žiadna kritická zraniteľnosť. V prehliadači Firefox bolo opravených 9 závažných zraniteľností, pričom 5 z nich sa vyskytuje aj v prehliadači Firefox ESR.

Závažná zraniteľnosť CVE-2021-29986 vyskytujúca sa v oboch prehliadačoch sa týka súbehu pri volaní funkcie „getaddrinfo“, čo môže viesť k poškodeniu pamäte. Chyba ovplyvňuje prehliadače v operačných systémoch Linux.

Ďalšia zraniteľnosť oboch prehliadačov CVE-2021-29988 súvisí s čítaním mimo povolených hodnôt. CVE-2021-29984 a CVE-2021-29980 môžu viesť k poškodeniu pamäte a následnému zlyhaniu prehliadača. CVE-2021-29989 sú chyby súvisiace s pamäťou v prehliadači Firefox 90 a Firefox ESR 78.12. S dostatočným úsilím by mohol útočník vzdialene vykonať kód.

V prehliadači Firefox sa vyskytuje závažná zraniteľnosť CVE-2021-29981, pričom môže viesť ku deterministickým chybám v JIT kóde.

V prehliadači Firefox pre Android sa vyskytuje zraniteľnosť CVE-2021-29983. Môže sa zaseknúť v režime celej obrazovky a neukončiť sa ani po bežných interakciách, ktoré by mali spôsobiť jeho ukončenie.

CVE-2021-29990 sú chyby pamäte v prehliadači Firefox verzie 90. S dostatočným úsilím by mohol útočník vzdialene vykonať kód.

Závažná zraniteľnosť CVE-2021-29991 sa vyskytuje v prehliadači Firefox verzie 91. Firefox nesprávne prijíma nový riadok v hlavičke typu HTTP/3 a interpretuje ho ako dve samostatné hlavičky. To umožňuje útoky voči serverom používajúcim protokol HTTP/3.

Zraniteľné systémy:
Mozilla Firefox pre Android verzie staršej ako 91.0.1
Mozilla Firefox ESR verzie staršej ako 78.13.

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 91.0.1 a Firefox ESR na verziu 78.13.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-33/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-34/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-37/

Google Chrome

V mesiaci august bola vydaná oprava pre 17 závažných zraniteľností. Zraniteľnosti sa väčšinou týkajú použitia odalokovaného miesta v pamäti, pretečenia medzipamäte haldy a zápisu alebo čítania mimo povolených hodnôt. Zraniteľnosti sa nachádzajú v komponentoch ako Web Share, V8, WebRTC, WebAudio, Blink a ďalších.

Zraniteľné systémy:
Google Chrome verzie staršej ako 93.0.4577.63

Odporúčania:
Odporúčame aktualizáciu na verziu 93.0.4577.63

Zdroje:
https://chromereleases.googleblog.com/2021
https://chromereleases.googleblog.com/2021/08/the-stable-channel-has-been-updated-to.html
https://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html

4. Adobe Acrobat a Reader

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

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

5. Frameworky

Microsoft .NET Framework

V mesiaci august spoločnosť Microsoft opravila 2 závažné zraniteľnosti vo frameworku .NET. Zneužitím CVE-2021-26423 môže dôjsť k narušeniu dostupnosti služby a zneužitím CVE-2021-34485 môže dôjsť k úniku informácií.

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/