Mesačný prehľad kritických zraniteľností
november 2021

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci november 3 kritické a 27 závažných zraniteľností.

Kritická zraniteľnosť CVE-2021-26443 sa nachádza v mechanizme Microsoft Virtual Machine Bus (VMBus). Umožňuje vzdialené vykonanie kódu v zraniteľnom systéme. Existuje z dôvodu nesprávneho overovania vstupu vo VMBus. Vzdialený útočník v lokálnej sieti môže odoslať špeciálne vytvorenú komunikáciu na VMBus kanál a následne vykonať ľubovoľný kód.

Ďalšia zraniteľnosť CVE-2021-38666 sa vyskytuje v klientovi vzdialenej plochy (Remote Desktop Client). V prípade, že sa používateľ pripojí pomocou zraniteľného klienta k serveru, ktorý je pod kontrolou útočníka, útočník by mohol vzdialene vykonávať kód na klientskom zariadení.

Posledná zraniteľnosť CVE-2021-42279 sa nachádza v skriptovacom nástroji Chakra. Zneužitím by mohlo dôjsť k poškodeniu pamäte a útočník by tak mohol vzdialene vykonávať ľubovoľný kód.

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 10 Version 21H1 for 32-bit Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows 10 Version 21H1 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, 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-2021-26443
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-38666
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-42279

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci november 6 závažných zraniteľností. Päť z nich (CVE-2021-40442, CVE-2021-41368, CVE-2021-42296, CVE-2021-43208 a CVE-2021-43209) umožňuje útočníkom vzdialené vykonávanie kódu. Zraniteľnosť CVE-2021-42292 môže viesť k obídeniu bezpečnostných prvkov.

Zraniteľné systémy:

3D Viewer
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 LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office LTSC for Mac 2021
Microsoft Office Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2013 Service Pack 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

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 november nebola v prehliadači Firefox a Firefox ESR opravená žiadna kritická zraniteľnosť. V prehliadači Firefox bolo opravených 7 závažných zraniteľností, pričom 6 z nich sa vyskytuje aj v prehliadači Firefox ESR. V prehliadači Firefox ESR sa vyskytuje okrem týchto 6 zraniteľností ešte 1 zraniteľnosť naviac.

CVE-2021-38503 vyskytujúca sa v oboch prehliadačoch súvisí s pravidlami pre testovacie prostredie (sandbox) iframe. Tieto neboli správne aplikované na šablóny so štýlmi XSLT, čo umožnilo testovaciemu prostrediu obísť obmedzenia.

CVE-2021-38504 sa týka použitia odalokovaného miesta v pamäti pri použití dialógového okna na výber súboru. Chyba môže viesť k poškodeniu pamäte a následne k zneužiteľnému zlyhaniu.

Závažná zraniteľnosť CVE-2021-38505 ovplyvňuje len Firefox pre Windows 10 a vyššie so zapnutou funkciou Cloud Clipboard. Aplikácie, ktoré chcú zabrániť zaznamenávaniu skopírovaných údajov do histórie cloudu, musia používať špecifické formáty pre schránku – Firefox pred verziami 94 a ESR 91.3 ich nemal implementované.

Zraniteľnosť CVE-2021-38506 spôsobovala, že Firefox mohol byť prinútený prejsť do režimu celej obrazovky bez akéhokoľvek varovania. To by mohlo viesť k útokom súvisiacim s predstieraním identity vrátane phishingu.

CVE-2021-38507 súvisí s funkcionalitou „oportunistické šifrovanie“ (Opportunistic Encryption) v HTTP2. Môže sa zneužiť na obídenie politiky Same-Origin-Policy v službách hostených na iných portoch.

MOZ-2021-003 sa vyskytuje len v prehliadači Firefox pre Android. Jedná sa o XSS zraniteľnosť v dôsledku nesprávnej sanitácie pri spracovávaní URL adries z QR kódov. MOZ-2021-007 nachádzajúce sa v prehliadači Firefox aj Firefox ESR sú chyby súvisiace s pamäťou. S dostatočným úsilím by mohol útočník vzdialene vykonať kód.

V prehliadači Firefox ESR sa vyskytuje chyba s označením MOZ-2021-0008. Použitie odalokovaného miesta v pamäti sa môže vyskytnúť, keď je objekt relácie HTTP2 uvoľnený pre iné vlákno, čo môže viesť k poškodeniu pamäte a následne k zneužitiu tejto zraniteľnosti.

Zraniteľné systémy:
Mozilla Firefox verzie staršej ako 94
Mozilla Firefox ESR verzie staršej ako 91.3

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 94 a Firefox ESR na verziu 91.3.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-48/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-49/

Google Chrome

V mesiaci november bola vydaná oprava pre 7 závažných zraniteľností. Zraniteľnosti sa väčšinou týkajú použitia odalokovaného miesta v pamäti a nesprávnej implementácie. Zraniteľnosti sa nachádzajú v komponentoch ako V8, loader, cache, media a ďalších.

Zraniteľné systémy:
Google Chrome verzie staršej ako 96.0.4664.45

Odporúčania:
Odporúčame aktualizáciu na verziu 96.0.4664.45

Zdroje:
https://chromereleases.googleblog.com/2021
https://chromereleases.googleblog.com/2021/11/stable-channel-update-for-desktop.html

4. Adobe Acrobat a Reader

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

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

5. Frameworky

Microsoft .NET Framework

V mesiaci november 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 18. január 2022.

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

6. Iné závažné zraniteľnosti

Zraniteľnosť WinRAR umožňuje vykonávať kód

Výskumníci spoločnosti Positive Technologies odhalili zraniteľnosť obľúbeného archivátora WinRAR. Dovoľujeodchytávať a upravovať požiadavky, ktoré aplikácia posiela používateľovi. Po splnení istých podmienok ju môžu útočníci zneužiť na vzdialené vykonávanie kódu na zariadení obete. Spoločnosť WinRAR chybu opravila v júli tohto roka. Viac informácií na stránke.

V serveroch Microsoft Exchange sa vyskytuje aktívne zneužívaná závažná zraniteľnosť

Spoločnosť Microsoft urguje používateľov, aby si aktualizovali svoje Exchange servery z dôvodu výskytu závažnej zraniteľnosti, ktorá je aktívne zneužívaná. Zneužitím môže dôjsť k vzdialenému vykonaniu ľubovoľného kódu autentifikovaným útočníkom v zraniteľnom systéme. Viac informácií na stránke.