Mesačný prehľad kritických zraniteľností december 2021

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci december 3 kritické a 35 závažných zraniteľností.

Kritická zraniteľnosť CVE-2021-43215 sa vyskytuje v serveri iSNS a súvisí s poškodením pamäte. Útočník môže odoslať špeciálne vytvorenú požiadavku na server iSNS, čo môže viesť k vzdialenému vykonaniu kódu. Windows iSNS nie je predvolene inštalovaný.

Ďalšia zraniteľnosť CVE-2021-43217 sa nachádza vo Windows Encrypting File System (EFS). Útočník môže spôsobiť zápis mimo povolených hodnôt a následne vykonať ľubovoľné príkazy v cieľovom systéme.

Posledná zraniteľnosť CVE-2021-43233 sa vyskytuje v klientovi vzdialenej plochy (Remote Desktop Client). Vzdialený útočník môže odoslať špeciálne vytvorenú požiadavku a následne vykonať kód v zraniteľnom systéme. Zneužitím by mohlo dôjsť k úplnej kompromitácii predmetného systému.

Zraniteľné systémy:

HEVC Video Extensions
Raw Image Extension
VP9 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 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, 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-2021-43215
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-43217
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-43233

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci december 1 kritickú a 11 závažných zraniteľností. Kritická zraniteľnosť CVE-2021-43905 sa nachádza v aplikácii Microsoft Office a môže viesť k vzdialenému vykonaniu kódu.

Štyri zo závažných zraniteľností (CVE-2021-42294, CVE-2021-42309, CVE-2021-43256 a CVE-2021-43875) umožňujú útočníkom vzdialené vykonávanie kódu. Zneužitím zraniteľností CVE-2021-42293 a CVE-2021-43876 môže dôjsť k eskalácii privilégií. Zraniteľnosť CVE-2021-42295 môže viesť k odhaleniu citlivých informácií. Posledné štyri zraniteľnosti

(CVE-2021-42320, CVE-2021-43242, CVE-2021-43255 a CVE-2021-43890) môžu dovoliť útočníkovi predstierať cudziu identitu.

Zraniteľné systémy:

App Installer
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 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 SharePoint Server Subscription Edition
Office app
Office Online Server
SharePoint Server Subscription Edition Language Pack

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-2021-43905

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 december nebola v prehliadači Firefox a Firefox ESR opravená žiadna kritická zraniteľnosť. V prehliadači Firefox bolo opravených 6 závažných zraniteľností, pričom 5 z nich sa vyskytuje aj v prehliadači Firefox ESR.

Nasledujúce zraniteľnosti sa vyskytujú v oboch prehliadačoch. CVE-2021-43536 súvisí s tým, že v istých prípadoch môžu asynchrónne funkcie spôsobiť odhalenie cieľovej URL. CVE-2021-43537 súvisí s nesprávnym spôsobom konverzie typu premennej zo 64-bitového na 32-bitový integer, čo môže viesť ku pretečeniu zásobníka haldy. CVE-2021-43538 sa týka súbehu v kóde pre notifikácie, čo umožňuje skryť notifikáciu pre stránky s prístupom k atribútom fullscreen a pointer lock. To dovoľuje útoky typu spoofing. CVE-2021-43539 je chyba v zaznamenávaní polohy ukazovateľov vo volaniach WebAssembly, čo môže viesť k použitiu odalokovaného miesta v pamäti.

CVE-2021-4129 vyskytujúca sa v prehliadačoch Firefox 94 a v Firefox ESR 91.3 je séria chýb zabezpečenia v pamäti, z ktorých niektoré majú potenciál zneužitia pre vykonávanie ľubovoľného kódu.

CVE-2021-4128 je chyba prítomná vo verzii Firefox pre MacOS umožňujúca použitie odalokovaného miesta v pamäti pri zmene okna z a na fullscreen.

Zraniteľné systémy:
Mozilla Firefox verzie staršej ako 95

Mozilla Firefox ESR verzie staršej ako 91.4.0

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 95 a Firefox ESR na verziu 91.4.0.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-52/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-53/

Google Chrome

V mesiaci december bola vydaná oprava pre 1 kritickú a 21 závažných zraniteľností.

Kritická zraniteľnosť CVE-2021-4096 súvisí s nedostatočným overovaním údajov v komponente Mojo. Závažné zraniteľnosti sa väčšinou týkajú použitia odalokovaného miesta v pamäti, pretečenia medzipamäte haldy a zapisovaním mimo povolených hodnôt. Zraniteľnosti sa nachádzajú v komponentoch ako V8, loader, UI, Swiftshader a ďalších.

Zraniteľné systémy:
Google Chrome verzie staršej ako 96.0.4664.110

Odporúčania:
Odporúčame aktualizáciu na verziu 96.0.4664.110

Zdroje:
https://chromereleases.googleblog.com/2021
https://chromereleases.googleblog.com/2021/12/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2021/12/stable-channel-update-for-desktop_13.html

4. Adobe Acrobat a Reader

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

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

5. Frameworky

Microsoft .NET Framework

V mesiaci december spoločnosť Microsoft opravila 1 závažnú zraniteľnosť vo frameworku .NET. Zneužitím zraniteľnosti CVE-2021-43877 môže dôjsť k eskalácii privilégií.

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

Zraniteľné systémy:
ASP.NET Core 3.1
ASP.NET Core 5.0

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.

Oracle Java

Veľká sada opráv je plánovaná na 18. január 2022.

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

6. Iné závažné zraniteľnosti

Spoločnosť HP opravila zraniteľnosti ovplyvňujúce minimálne 150 modelov multifunkčných tlačiarní

Zraniteľnosti sa v asi 150 modeloch multifunkčných zariadení spoločnosti HP (Hewlett Packard) vyskytujú už od roku 2013. Nahlásené a opravené však boli až v roku 2021. Útočníci ich môžu zneužiť na krádež informácií alebo vzdialené vykonanie kódu. Na opravu týchto chýb je nutné aktualizovať firmvér. Viac informácií na stránke.

Závažná zraniteľnosť platformy WordPress umožňuje útoky cez distribučný kanál pluginov a tém

Obľúbená platforma na tvorbu webových stránok obsahuje závažnú zraniteľnosť, ktorá útočníkom umožňuje jednoduchým spôsobom vymeniť tému či plugin webstránky za jeho škodlivú verziu. To môže viesť ku vzdialenému vykonávaniu kódu a kompromitácii webstránky. Ak stránka používa vlastný neregistrovaný doplnok, útočníkovi stačí zaregistrovať svoj plugin na webe wordpress.org s rovnakým názvom. V rámci automatickej aktualizácie si následne stránka stiahne škodlivú verziu. Viac informácií na stránke.

Zraniteľnosť CVE-2021-44228 (Log4Shell)

Dňa 9.12.2021 bola zverejnená informácia o zraniteľnosti knižnice Log4j vo verzii 2 od spoločnosti The Apache Software Foundation. Zraniteľnosť s označením CVE-2021-44228 (Log4Shell, LogJam) a vysokou závažnosťou umožňuje vzdialené spustenie kódu. Viac informácií na stránke.

V zariadeniach SMA spoločnosti SonicWall sa vyskytuje 8 zraniteľností

Spoločnosť SonicWall opravila 8 zraniteľností v zariadeniach Secure Mobile Access (SMA) série 100, z čoho 2 sú kritické, 4 závažné a 2 stredne závažné. Dôsledkom zneužitia týchto zraniteľností môže byť vzdialené vykonanie kódu na zraniteľnom zariadení. Viac informácií na stránke.