Mesačný prehľad kritických zraniteľností
október 2021

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci október 2 kritické a 45 závažných zraniteľností.

Obe kritické zraniteľnosti (CVE-2021-38672 a CVE-2021-40461) sa nachádzajú vo Windows Hyper-V. Umožňujú vzdialenému útočníkovi vykonať ľubovoľný kód v zraniteľnom systéme. Existujú z dôvodu nesprávneho overovania vstupu vo Windows Hyper-V. Vzdialený autentifikovaný útočník môže v lokálnej sieti poslať špeciálne vytvorenú požiadavku a vykonať ľubovoľný kód v cieľovom systéme. Úspešným zneužitím týchto zraniteľností by mohlo dôjsť k úplnej kompromitácii systému.

Zraniteľné systémy:

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-2021-40461
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-38672

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci október 1 kritickú a 14 závažných zraniteľností. Kritická zraniteľnosť CVE-2021-40486 sa nachádza v produkte Microsoft Word. Súvisí s použitím odalokovaného miesta v pamäti pri spracovávaní .doc súborov. Vzdialený útočník môže nalákať obeť na otvorenie špeciálne vytvoreného súboru a následne vykonať ľubovoľný kód v systéme. Úspešným zneužitím by mohlo dôjsť k úplnej kompromitácii zraniteľného systému.

Deväť zo závažných zraniteľností (CVE-2021-40471, CVE-2021-40473, CVE-2021-40474, CVE-2021-40479, CVE-2021-40480, CVE-2021-40481, CVE-2021-40485, CVE-2021-40487 a CVE-2021-41344) umožňuje útočníkom vzdialené vykonávanie kódu. Zneužitím zraniteľnosti CVE-2021-40484 môže dôjsť k predstieraniu identity. Zraniteľnosť CVE-2021-41363 môže viesť k obídeniu bezpečnostných prvkov. Zneužitie závažných zraniteľností CVE-2021-40454, CVE-2021-40472 a CVE-2021-40482 môže spôsobiť únik informácií.

Zraniteľné systémy:

Intune management extension
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
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2019
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 Service Pack 1 (64-bit editions)
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
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-40486

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 september 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.

CVE-2021-38496 vyskytujúca sa v oboch prehliadačoch súvisí s použitím odalokovaného miesta v pamäti. Počas operácií v MessageTasks môže byť odstránená úloha (ktorá bola naplánovaná), čo môže viesť k poškodeniu pamäte.

CVE-2021-38500 a CVE-2021-38501 nachádzajúce sa v prehliadači Firefox aj Firefox ESR sú chyby súvisiace s pamäťou. S dostatočným úsilím by mohol útočník vzdialene vykonať kód. Chyby s označením CVE-2021-38499 v prehliadači Firefox taktiež súvisia s pamäťou. Niektoré z týchto chýb spôsobovali poškodenie pamäte a tiež by mohli byť zneužité na vykonanie ľubovoľného kódu.

V prehliadači Firefox sa taktiež 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 93
Mozilla Firefox ESR verzie staršej ako 91.2
Mozilla Firefox ESR verzie staršej ako 78.15

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 93 a Firefox ESR na verziu 91.2 alebo 78.15.

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

https://www.mozilla.org/en-US/security/advisories/mfsa2021-43/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-44/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-45/

Google Chrome

V mesiaci október bola vydaná oprava pre 16 závažných zraniteľností. Zraniteľnosti sa väčšinou týkajú použitia odalokovaného miesta v pamäti, nesprávnej implementácie a pretečenia medzipamäte haldy. Zraniteľnosti sa nachádzajú v komponentoch ako Blink, WebRTC, PDFium, Skia a ďalších.

Zraniteľné systémy:
Google Chrome verzie staršej ako 95.0.4638.69

Odporúčania:
Odporúčame aktualizáciu na verziu 95.0.4638.69

Zdroje:
https://chromereleases.googleblog.com/2021
https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html
https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html

4. Adobe Acrobat a Reader

V produkte Adobe Acrobat a Reader boli opravené 2 kritické zraniteľnosti. Kritická zraniteľnosť CVE-2021-40728 súvisí s použitím odalokovaného miesta v pamäti. Zneužitím sú útočníci schopní vzdialene vykonávať ľubovoľný kód. Zraniteľnosť CVE-2021-39852 sa týka zápisu mimo povolených hodnôt a zneužitím môže dôjsť k vykonaniu ľubovoľného kódu.

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

Odporúčania:
Odporúčame aktualizáciu:
Acrobat DC na verziu 21.007.20099
Acrobat Reader DC na verziu 21.007.20099
Acrobat 2020 na verziu 20.004.30017
Acrobat Reader 2020 na verziu 20.004.30017
Acrobat 2017 na verziu 17.011.30204
Acrobat Reader 2017 na verziu 17.011.30204

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/acrobat/apsb21-104.html

5. Frameworky

Microsoft .NET Framework

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

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

Oracle Java

Spoločnosť Oracle vydala v mesiaci október plánovanú štvrťročnú veľkú sadu aktualizácií. V Oracle Java SE bolo dokopy opravených 15 zraniteľností, z čoho 3 boli závažné.

Závažné zraniteľnosti CVE-2021-3517 a CVE-2021-35560 sa vyskytujú v produkte Java SE, pričom sa vzťahujú na nasadenia programovacieho jazyka Java, zvyčajne v klientoch, ktorí používajú karanténne aplikácie Java Web Start alebo Java aplety. Tieto načítavajú a spúšťajú nedôveryhodný kód (napríklad kód pochádzajúci z internetu). K zneužitiu týchto chýb môže dôjsť bez autentifikácie útočníka.

Zraniteľnosť CVE-2021-27290 sa nachádza v Oracle GraalVM Enterprise Edition v komponente „Node.js“ a umožňuje spôsobiť odmietnutie služby. K zneužitiu tejto chyby môže dôjsť bez autentifikácie útočníka.

Zraniteľné systémy:
Java SE: 7u311, 8u301, 11.0.12, 17

Oracle GraalVM Enterprise Edition: 20.3.3, 21.2.0

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/cpuoct2021.html

6. Iné závažné zraniteľnosti

Kritická zraniteľnosť produktu VMware VCenter

Spoločnosť WMware varuje pred kritickou zraniteľnosťou svojho produktu VMware vCenter. Chyba sa nachádza v nástroji VMware Analytics, ktorý dokáže prijať škodlivý súbor bez akejkoľvek autentifikácie, zapísať ho kdekoľvek na disk a následne spustiť s oprávneniami správcu. Zraniteľnosť je triviálne zneužiteľná a preto VMware apeluje na administrátorov systémov VMware, aby bezodkladne vykonali kroky k zabezpečeniu svojej infraštruktúry. Aktuálne je postup zneužitia zraniteľnosti už voľne dostupný na internete. Viac informácií na stránke.

Kritická zraniteľnosť Apache HTTP server

Apache Software Foundation vydala dôležité opravy kritickej zraniteľnosti, ktorá umožňuje potenciálnemu útočníkovi odosielať požiadavky a získať prístup k súborom na backende webového servera. Zraniteľnosť sa nachádza len vo verzii Apache 2.4.49. Úspešným zneužitím zraniteľnosti môže prísť k úniku binárnych súborov ako sú napríklad CGI skripty, či zmapovaniu súborov mimo publikovaných web root súborov. Zraniteľnosť je aktívne zneužívaná útočníkmi. CSIRT.SK odporúča bezodkladnú aktualizáciu zraniteľných systémov. Viac informácií na stránke.