Mesačný prehľad kritických zraniteľností
február 2021

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci február 9 kritických a 19 závažných zraniteľností. Všetky kritické zraniteľnosti môžu viesť k vzdialenému vykonávaniu kódu.

Kritické zraniteľnosti CVE-2021-1722 a CVE-2021-24077 sa nachádzajú v službe pre fax a skenovanie. Aby bolo možné tieto chyby zneužiť, je potrebné mať povolenú funkciu Windows Fax a skenovanie a musí byť spustená služba Fax. Systémy, ktoré nemajú spustenú túto službu, nie sú zraniteľné.

Zraniteľnosti CVE-2021-24074 a CVE-2021-24094 súvisia s implementáciou TCP/IP. Zneužitie týchto chýb je z krátkodobého hľadiska nepravdepodobné, pretože vyžaduje zložitý proces (v dlhšom časovom horizonte však spoločnosť zneužívanie týchto zraniteľností očakáva). Útočníci však môžu vyvinúť útoky typu DoS, čo by im umožnilo spôsobiť chybu zastavenia. Na zneužitých zariadeniach sa preto môže vyskytnúť pád systému do tzv. „blue screen of death“.

Ďalšia kritická zraniteľnosť CVE-2021-24078 súvisí so serverom Windows DNS. Zneužitím tejto zraniteľnosti je útočník schopný vzdialene vykonávať ľubovoľný kód.

Kritické zraniteľnosti CVE-2021-24081 v Microsoft Windows Codecs Library, CVE-2021-24088 v nástroji Windows Local Spooler a CVE-2021-24091 vo Windows Camera Codec Pack súvisia s nedostatočným overením vstupu zadaného používateľom. Vzdialený útočník môže vytvoriť špeciálny vstup pre aplikáciu a následne vykonávať ľubovoľný kód v zraniteľnom systéme.

Posledná zraniteľnosť CVE-2021-24093 súvisí s komponentom Windows Graphics. Útočník by mohol byť hostiteľom webovej stránky, ktorá obsahuje špeciálne vytvorený súbor na zneužitie tejto chyby. V iných prípadoch by útočník musel presvedčiť používateľa, aby klikol na odkaz, zvyčajne pomocou podvrhnutého emailu, a následne otvoril špeciálne vytvorený súbor.

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 1803 for 32-bit Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows 10 Version 1803 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 1903 for 32-bit Systems
Windows 10 Version 1903 for ARM64-based Systems
Windows 10 Version 1903 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 1903 (Server Core installation)
Windows Server, version 1909 (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-2021-1722
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-24074
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-24077
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-24078
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-24081
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-24088
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-24091
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-24093

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-24094

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci február 11 závažných a žiadnu kritickú zraniteľnosť.

Zraniteľnosti CVE-2021-24066 až CVE-2021-24070 a CVE-2021-24072 umožňujú útočníkom vzdialené vykonávanie kódu. Zneužitím zraniteľností CVE-2021-1726 a CVE-2021-24073 môže dôjsť k predstieraniu cudzej identity. Zraniteľnosť CVE-2021-24099 môže spôsobiť narušenie dostupnosti služby. Zraniteľnosti CVE-2021-24071 v produktoch SharePoint a CVE-2021-24114 v Microsoft Teams pre iOS môžu viesť k vyzradeniu informácií.

Zraniteľné systémy:

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Excel 2010 Service Pack 2 (32-bit editions)
Microsoft Excel 2010 Service Pack 2 (64-bit editions)
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 Lync Server 2013
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 2010 Service Pack 2
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2019
Microsoft Teams for iOS
Office Online Server
Skype for Business Server 2015 CU 8
Skype for Business Server 2019 CU2

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 v mesiaci február 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 Microsoft Edge jednu závažnú zraniteľnosť a žiadnu kritickú zraniteľnosť. Závažná zraniteľnosť CVE-2021-24113 môže viesť k obídeniu bezpečnostných prvkov. Umožňuje pri kopírovaní a vkladaní do prehliadača Edge vykonávať Javascript v URL.

Zraniteľné systémy:
Microsoft Edge (EdgeHTML-based)

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

Mozilla Firefox

V mesiaci február bola v prehliadači Firefox a Firefox ESR opravená jedna kritická zraniteľnosť. V prehliadači Firefox bolo opravených 5 závažných zraniteľností, pričom 3 z nich sa vyskytujú aj vo Firefox ESR.

Kritická zraniteľnosť v oboch produktoch s označením MOZ-2021-0001 súvisí s pretečením medzipamäte pri výpočtoch hĺbkových rozsahov pre komprimované textúry. Zraniteľnosť sa

nachádza v grafickej knižnici Angle. Táto chyba ovplyvňuje len operačné systémy Windows. Zraniteľnosť čaká na priradenie identifikátora CVE.

Závažné zraniteľnosti môžu viesť k poškodeniu pamäte, k vykonávaniu ľubovoľného kódu a k úniku údajov.

Zraniteľné systémy:
Mozilla Firefox verzie staršej ako 86
Mozilla Firefox ESR verzie staršej ako 78.8

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 86 resp. Firefox ESR na 78.8.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-06/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-07/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-08/

Google Chrome

V mesiaci február bola vydaná oprava pre 1 kritickú a 13 závažných zraniteľností. Kritická zraniteľnosť CVE-2021-21142 súvisí s použitím odalokovaného miesta v pamäti. Nachádza sa v komponente Payments v prehliadači Chrome. Umožňuje vzdialenému útočníkovi vykonávať ľubovoľný kód a kompromitáciu zraniteľného systému.

Závažné zraniteľnosti sa väčšinou týkajú pretečenia medzipamäte haldy, použitia odalokovaného miesta v pamäti alebo nevhodnej implementácie.

Zraniteľné systémy:
Google Chrome verzie staršej ako 88.0.4324.192 pre Mac a Linux
Google Chrome verzie staršej ako 88.0.4324.190 pre Windows

Odporúčania:
Odporúčame aktualizáciu na verziu 88.0.4324.192 pre Mac a Linux a na verziu 88.0.4324.190 pre Windows.

Zdroje:
https://chromereleases.googleblog.com/2021

https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_4.html
https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html
https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_22.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci február bola vydaná oprava pre 17 kritických a 6 závažných zraniteľností v produkte Adobe Acrobat a Reader. Adobe prestal vydávať záplaty pre Flash Player 31. decembra 2020, teda nie je bezpečné ho používať.

Kritické zraniteľnosti CVE-2021-21041, CVE-2021-21040, CVE-2021-21039, CVE-2021-21035, CVE-2021-21033, CVE-2021-21028 a CVE-2021-21021 súvisia s použitím odalokovaného miesta v pamäti a môžu viesť ku vzdialenému vykonaniu kódu.

CVE-2021-21058, CVE-2021-21059, CVE-2021-21062 a CVE-2021-21063 súvisia s pretečením medzipamäte. Zneužitím sú útočníci schopní vzdialene vykonávať ľubovoľný kód. CVE-2021-21036 sa týka pretečenia premennej typu integer. CVE-2021-21017 súvisí s pretečením medzipamäte haldy.

CVE-2021-21044 a CVE-2021-21038 sú zraniteľnosti súvisiace so zápisom mimo povolených hodnôt. CVE-2021-21037 umožňuje útočníkom čítať súbory. CVE-2021-21045 súvisí s nesprávnou kontrolou prístupu.

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

Odporúčania:
Odporúčame aktualizáciu:
Acrobat DC na verziu 2021.001.20135
Acrobat Reader DC na verziu 2021.001.20135
Acrobat 2020 na verziu 2020.001.30020

Acrobat Reader 2020 na verziu 2020.001.30020
Acrobat 2017 na verziu 2017.011.30190
Acrobat Reader 2017 na verziu 2017.011.30190

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/acrobat/apsb21-09.html

5. Frameworky

Microsoft .NET Framework

V mesiaci február spoločnosť Microsoft vydala opravnú aktualizáciu pre 2 kritické a 2 závažné zraniteľnosti vo frameworku .NET. Kritické zraniteľnosti CVE-2021-24112 a CVE-2021-26701 môžu viesť ku vzdialenému vykonávaniu kódu.

Zraniteľné systémy:
.NET 5.0
.NET Core 2.1
.NET Core 3.1
Microsoft .NET Framework 4.6
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 4.7.2
Microsoft .NET Framework 4.8

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-2021-24112
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-26701

Oracle Java

Veľká sada opráv je plánovaná na 20. apríl 2021.

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

6. Iné závažné zraniteľnosti

Závažná zraniteľnosť v knižnici GnuPG Libgcrypt

V knižnici GnuPG Libcrypt existuje vysoko závažná zraniteľnosť v spôsobe dešifrovania dát. Útočníkom umožňuje spôsobiť zrútenie aplikácie, ktorá knižnicu používa, alebo vzdialene vykonávať kód. Toto je možné dosiahnuť jednoducho dešifrovaním špeciálne upraveného balíka dát. Viac informácií na stránke.

Spoločnosť Cisco vydala bezpečnostné aktualizácie pre svoje produkty

Spoločnosť Cisco vydala bezpečnostné aktualizácie na opravu kritických zraniteľností, ktoré môžu byť zneužite na vzdialené vykonanie kódu (RCE) v produktoch SD-WAN, aplikácií Cisco DNA Center a softvéri na správu licencii (Smart Software Manager). Spoločnosť Cisco apeluje na čo najrýchlejšiu aktualizáciu zraniteľných produktov. Viac informácií na stránke.

Baron Samedit: eskalácia privilégií v linuxovom nástroji Sudo

V programe Sudo, ktorý umožňuje vykonávať vybrané operácie s právami používateľa root v operačných systémoch Unix/Linux, bola opravená kritická zraniteľnosť. Nazvaná ako „Baron Samedit“ bola objavená bezpečnostnou auditnou spoločnosťou Qualys a umožňuje získať oprávnenia používateľa root každému lokálnemu používateľovi. Zraniteľnosť sa v programe Sudo nachádzala 9 rokov. Viac informácií na stránke.

Spoločnosť Apple opravila závažné bezpečnostné zraniteľnosti v operačnom systéme iOS a iPadOS. Tri sú aktívne zneužívané.

Spoločnosť Apple vydala aktualizáciu, ktorá opravila aj 3 závažné zero-day zraniteľnosti, ktoré by mohli byť zneužité na kompromitáciu zariadenia vzdialeným útočníkom a vzdialené vykonávanie kódu. Zraniteľnosti sa nachádzajú v jadre operačného systému a v platforme webového prehľadávania WebKit. Viac informácií na stránke.

Spoločnosť Cisco opravila 9 zraniteľností vo webovom rozhraní pre správu VPN smerovačov

Spoločnosť Cisco vydala opravu 9 zraniteľností vo webovom rozhraní pre správu VPN smerovačov, z čoho 7 je kritických a 2 závažné. Chyby vo všeobecnosti útočníkovi umožňujú vzdialené vykonávanie kódu na dotknutých zariadeniach. Kritické súvisia s nesprávnym overovaním HTTP požiadaviek a závažné sú spôsobené nedostatočným overovaním vstupu. Viac informácií na stránke.

V komponente V8 prehliadača Chrome bola opravená aktívne zneužívaná zero-day zraniteľnosť

V prehliadači Chrome spoločnosti Google bola opravená aktívne zneužívaná zraniteľnosť, ktorá existuje v komponente V8. Jedná sa o pretečenie medzipamäte haldy. Spoločnosť Google zatiaľ nezverejnila viac informácií. Chce počkať, kým si väčšina používateľov nainštaluje najnovšiu dostupnú aktualizáciu. Viac informácií na stránke.