Mesačný prehľad kritických zraniteľností
november 2020

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci november 12 kritických a 54 závažných zraniteľností.

Chyba v operačných systémoch Windows CVE-2020-17042 súvisí so softvérom, ktorý spravuje požiadavky na tlač posielané do tlačiarne alebo na tlačový server. Ďalšia kritická zraniteľnosť CVE-2020-17051 súvisí so sieťovým súborovým systémom v operačnom systéme Windows.

CVE-2020-17078, CVE-2020-17079 a CVE-2020-17082 súvisia s rozšírením Raw Image. Zraniteľnosť CVE-2020-17101 sa týka rozšírenia HEIF Image. CVE-2020-17105 sa nachádza v rozšírení AV1 Video. Kritické zraniteľnosti CVE-2020-17106 až CVE-2020-17110 sa týkajú rozšírení HEVC Video.

Všetky tieto zraniteľnosti môžu viesť k vzdialenému vykonávaniu kódu.

Zraniteľné systémy:
AV1 Video Extension
HEIF Image Extension
HEVC Video Extensions
Raw Image Extension
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-2020-17042
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17051
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17078
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17079
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17082
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17101
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17105
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17106
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17107
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17108
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17109
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17110

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci november 14 závažných zraniteľností a žiadnu kritickú v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Sedem zo závažných zraniteľností môže viesť k vzdialenému vykonávaniu kódu, zneužitím ďalších dvoch môže dôjsť k vyzradeniu informácií. Ďalšie dve zraniteľnosti môžu viesť k obídeniu bezpečnostných prvkov a zvyšné tri môžu útočníkom umožniť úspešnú imitáciu identity iného odosielateľa.

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 Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2013 RT Service Pack 1
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 Online Server
Microsoft Office Web Apps 2013 Service Pack 1
Microsoft SharePoint Enterprise 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 2010 Service Pack 2
Microsoft SharePoint Server 2019
Microsoft Teams
Microsoft Word 2010 Service Pack 2 (32-bit editions)
Microsoft Word 2010 Service Pack 2 (64-bit editions)
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

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft opravila tento mesiac v prehliadači Internet Explorer 3 kritické zraniteľnosti.

Kritické zraniteľnosti CVE-2020-17052, CVE-2020-17053 a CVE-2020-17058 umožňujú vzdialenému útočníkovi vykonávať ľubovoľný kód v cieľovom systéme. Tieto chyby môžu viesť ku poškodeniu pamäte. Úspešným zneužitím môže dôjsť ku kompromitácii zraniteľného systému.

Zraniteľné systémy:
Microsoft Internet Explorer verzie 11

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-2020-17052
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17053
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17058

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac v prehliadači Microsoft Edge 3 kritické zraniteľnosti.

Tieto kritické zraniteľnosti v prehliadači Microsoft Edge môžu viesť k vzdialenému vykonávaniu kódu v cieľovom systéme. Útočník je schopný kompromitovať celé zariadenie a tiež môže dôjsť k poškodeniu pamäte.

Zraniteľné systémy:

Microsoft Edge (EdgeHTML-based) v systémoch Windows 10

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-2020-17048
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17052
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17058

Mozilla Firefox

V mesiaci november bola v prehliadači Firefox a Firefox ESR opravená 1 kritická zraniteľnosť. V najnovšej verzii Firefox boli opravené 4 závažné zraniteľnosti a vo Firefox ESR 2 závažné zraniteľnosti.

Kritická zraniteľnosť CVE-2020-26950 sa vyskytuje v prehliadači Firefox verzie 82.0.3, a Firefox ESR verzie 78.4.1. Jedná sa o použitie odalokovaného miesta v pamäti, čo môže viesť k úplnej kompromitácii zraniteľného systému.

Zraniteľné systémy:

Mozilla Firefox verzie staršej ako 83
Mozilla Firefox ESR verzie staršej ako 78.5

Odporúčania:

Odporúčame aktualizáciu Firefox na verziu 83 resp. Firefox ESR na 78.5.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-49/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-50/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-51/

Google Chrome

V mesiaci november bola vydaná oprava pre 20 závažných zraniteľností. Nebola opravená žiadna kritická zraniteľnosť. Vo veľkej miere sa jedná o nesprávnu implementáciu rôznych komponentov pre prehliadač Chrome alebo o použitie odalokovaného miesta v pamäti.

Zraniteľné systémy:
Google Chrome verzie staršej ako 87.0.4280.66 pre Windows a Linux
Google Chrome verzie staršej ako 87.0.4280.67 pre Mac

Odporúčania:
Odporúčame aktualizáciu na verziu 87.0.4280.66 pre Windows a Linux a na verziu 87.0.4280.67 pre Mac.

Zdroje:
https://chromereleases.googleblog.com/2020
https://chromereleases.googleblog.com/2020/11/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2020/11/stable-channel-update-for-desktop_9.html
https://chromereleases.googleblog.com/2020/11/stable-channel-update-for-desktop_11.html
https://chromereleases.googleblog.com/2020/11/stable-channel-update-for-desktop_17.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci november boli v Adobe Acrobat a Reader opravené 4 kritické a 6 závažných zraniteľností. Kritické zraniteľnosti môžu viesť k vzdialenému vykonávaniu ľubovoľného kódu. Spoločnosť Adobe nevydala opravu žiadnych kritických zraniteľností pre Adobe Flash Player.

Zraniteľné systémy:
Acrobat DC

Acrobat Reader DC
Acrobat 2020
Acrobat Reader 2020
Acrobat 2017
Acrobat Reader 2017

Odporúčania:
Odporúčame aktualizáciu:
Acrobat DC na verziu 2020.013.20064
Acrobat Reader DC na verziu 2020.013.20064
Acrobat 2020 na verziu 2020.001.30010
Acrobat Reader 2020 na verziu 2020.001.30010
Acrobat 2017 na verziu 2017.011.30180
Acrobat Reader 2017 na verziu 2017.011.30180

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/acrobat/apsb20-67.html

5. Frameworky

Microsoft .NET Framework

V mesiaci november spoločnosť Microsoft nevydala žiadnu opravnú aktualizáciu pre kritické či závažné zraniteľnosti vo frameworku Microsoft .NET.

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

Oracle Java

Veľká sada opráv je plánovaná na 19. január 2021.

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

6. Iné závažné zraniteľnosti

Spoločnosť Oracle dodatočne po vydaní plánovanej štvrťročnej aktualizácie opravila kritickú zraniteľnosť

Spoločnosť Oracle vydala záplatu na kritickú zraniteľnosť, ktorá umožňuje vzdialené vykonávanie kódu. Ovplyvňuje niekoľko verzií servera Oracle WebLogic. Môže byť zneužitá prostredníctvom protokolu HTTP bez autentifikácie. Viac informácií na stránke.

Spoločnosť Google opravila niekoľko zraniteľností v prehliadači Chrome, pričom dve z nich sú typu zero-day

Spoločnosť Google vydala záplatu pre niekoľko chýb zabezpečenia. Dve z nich sú typu zero-day, pričom zneužitie prvej môže viesť ku vzdialenému vykonávaniu kódu. Táto zraniteľnosť sa nachádza v komponente V8 pre prehliadač Chrome, pričom súvisí s jeho nesprávnou implementáciou. Ďalšia zero-day zraniteľnosť sa nachádza v prehliadači Chrome pre systém Android. Môže spôsobiť pretečenie medzipamäte haldy. Viac informácií na stránke.

Spoločnosť Apple vydala záplatu pre tri zero-day zraniteľnosti ovplyvňujúce rôzne druhy zariadení

Bezpečnostný tím spoločnosti Google odhalil tri zero-day zraniteľnosti v zariadeniach od spoločnosti Apple. Prvá zraniteľnosť sa týka knižnice FontParser, pričom môže viesť k poškodeniu pamäte, ďalšia súvisí s eskaláciou privilégií v jadre iOS, čo umožňuje vykonávanie ľubovoľného kódu a posledná môže viesť k úniku pamäte. Viac informácií na stránke.

Spoločnosť Oracle opravila 402 zraniteľností v októbrových aktualizáciách

Softvérová spoločnosť Oracle vydala v októbri množstvo aktualizácií, ktoré opravujú až 402 chýb v jej produktoch. Dvojica chýb (CVE-2020-1953 a CVE-2020-14871) dosiala skóre CVSS 10, kritických je aj mnoho ďalších chýb. Ako uvádza portál Threatpost.com, viac ako polovicu zraniteľností je možné zneužiť na diaľku bez autentifikácie. Viac informácií na stránke.

Za posledné tri týždne spoločnosť Google opravila už štvrtú a piatu zero-day zraniteľnosť v prehliadači Chrome

Závažné zraniteľnosti sa nachádzajú v prehliadači Chrome. CVE-2020-16013 súvisí s nesprávnou implementáciou komponentu V8, pričom môže viesť k vzdialenému vykonávaniu kódu. CVE-2020-16017 sa týka komponentu, ktorý slúži na izoláciu údajov rôznych webových

stránok a jej zneužitie môže spôsobiť poškodenie pamäte a umožniť vykonávanie ľubovoľného kódu. Viac informácií na stránke.

V IOS XR od spoločnosti Cisco sa nachádza zraniteľnosť, ktorej zneužitie môže viesť k nefunkčnosti smerovačov Cisco ASR série 9000

Zraniteľnosť nachádzajúca sa v IOS XR verzie nižšej ako 6.7.2 alebo 7.1.2 umožňuje vzdialeným útočníkom znefunkčniť smerovače Cisco ASR série 9000. Chyba vzniká nesprávnym pridelením prostriedkov pri spracovávaní sieťového prenosu a vo všeobecnosti môže viesť k narušeniu dostupnosti služby. Viac informácií na stránke.

V aplikácii Cisco Security Manager sa vyskytujú tri zraniteľnosti. Na dve z nich vydala spoločnosť záplatu.

Spoločnosť Cisco vydala záplatu na dve z troch objavených zraniteľností v aplikácii Cisco Security Manager. Obe opravené zraniteľnosti môžu útočníkovi umožniť neoprávnený prístup k citlivým údajom. Posledná neopravená zraniteľnosť sa týka Java funkcie, ktorá slúži na deserializáciu obsahu dodávaného používateľom. V prípade zneužitia je útočník schopný vzdialene vykonávať kód. Viac informácií na stránke.

V produktoch spoločnosti VMware bola odhalená kritická a závažná zraniteľnosť

V produktoch ESXi, Fusion, Workstation a VMware Cloud Foundation sa vyskytuje zraniteľnosť, ktorá sa týka použitia odalokovaného miesta v pamäti. Ovplyvňuje XHCI USB kontrolér, pričom jej zneužitie môže viesť k vykonávaniu ľubovoľného kódu na cieľovom systéme. Ďalšia chyba v produktoch spoločnosti VMware sa týka spôsobu správy systémových volaní a jej zneužitie môže viesť k zmene oprávnení v systéme. Viac informácií na stránke.