Mesačný prehľad kritických zraniteľností apríl 2021

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci apríl 14 kritických a 67 závažných zraniteľností. Všetky kritické zraniteľnosti môžu viesť ku vzdialenému vykonávaniu kódu.

Zraniteľnosti CVE-2021-27095 a CVE-2021-28315 sa nachádzajú v dekóderi Microsoft Windows Media Video. Existujú v dôsledku nesprávneho overenia vstupu. Vzdialený útočník môže oklamať obeť, aby otvorila špeciálne vytvorený súbor a následne bol vykonaný v systéme ľubovoľný kód.

Kritické zraniteľnosti CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339 a CVE-2021-28343 sa vyskytujú v Remote Procedure Call Runtime. Tiež súvisia s nesprávnym overením vstupu. Vzdialený útočník môže poslať špeciálne vytvorenú požiadavku a vykonať ľubovoľný kód v cieľovom systéme. Úspešným zneužitím týchto chýb môže dôjsť k úplnej kompromitácii zraniteľného systému.

Zraniteľné systémy:

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 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 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-2021-27095
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28315
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28329
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28330
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28331
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28332
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28333
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28334
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28335
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28336
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28337
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28338
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28339
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28343

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci apríl 7 závažných zraniteľností a žiadnu kritickú zraniteľnosť. Päť zo závažných zraniteľností (CVE-2021-28449, CVE-2021-28451, CVE-2021-28452, CVE-2021-28453 a CVE-2021-28454) umožňuje útočníkom vzdialené vykonávanie

kódu. Zneužitím zraniteľnosti CVE-2021-28450 v produktoch SharePoint môže dôjsť k nedostupnosti služby. Zraniteľnosť CVE-2021-28456 môže viesť k úniku 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 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 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 2010 Service Pack 2
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft Outlook 2010 Service Pack 2 (32-bit editions)
Microsoft Outlook 2010 Service Pack 2 (64-bit editions)
Microsoft Outlook 2013 RT Service Pack 1
Microsoft Outlook 2013 Service Pack 1 (32-bit editions)
Microsoft Outlook 2013 Service Pack 1 (64-bit editions)
Microsoft Outlook 2016 (32-bit edition)
Microsoft Outlook 2016 (64-bit edition)
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2010 Service Pack 2
Microsoft SharePoint Server 2010 Service Pack 2
Microsoft SharePoint Server 2019
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 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 Microsoft Edge žiadnu kritickú ani závažnú zraniteľnosť.

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

Mozilla Firefox

V mesiaci apríl nebola v prehliadači Firefox a Firefox ESR opravená žiadna kritická zraniteľnosť. V prehliadači Firefox boli opravené 4 závažné zraniteľnosti, pričom 2 z nich sa vyskytujú aj vo verzii Firefox ESR.

Závažná zraniteľnosť CVE-2021-23994 vyskytujúca sa v oboch prehliadačoch súvisí s tým, že WebGL framebuffer nie je včas inicializovaný. Môže viesť k poškodeniu pamäte, pričom môže spôsobiť zápis mimo povolených hodnôt. Druhá spoločná zraniteľnosť CVE-2021-23995 existuje, keď je povolený mód Responsive Design. Používa odkazy na objekty, ktoré boli predtým uvoľnené. S dostatočným vynaloženým úsilím by mohol útočník vzdialene vykonávať kód.

CVE-2021-23996 súvisí s tým, že použitím 3D CSS v spojení s Javascriptom môže byť obsah vykreslený mimo zobrazenú webovú stránku. Môže viesť k možnosti predstierať cudziu identitu. Posledná zraniteľnosť CVE-2021-23997 súvisí s neočakávanou konverziou dátových typov. Môže dôjsť k použitiu odalokovaného miesta v pamäti. S dostatočne vynaloženým úsilím by mohol útočník taktiež vzdialene vykonávať kód.

Zraniteľné systémy:
Mozilla Firefox verzie staršej ako 88
Mozilla Firefox ESR verzie staršej ako 78.10

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 88 resp. Firefox ESR na 78.10.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-15/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-16/

Google Chrome

V mesiaci apríl bola vydaná oprava pre 16 závažných zraniteľností a žiadnu kritickú. Závažné zraniteľnosti sa väčšinou týkajú použitia odalokovaného miesta v pamäti, nedostatočného overovania dát, pretečenia medzipamäte haldy alebo prístupu k pamäti mimo povolených hodnôt. Zraniteľnosti sa vo veľkej miere nachádzajú v komponentoch V8, Blink a Mojo.

Zraniteľné systémy:
Google Chrome verzie staršej ako 90.0.4430.93 pre Windows, Mac a Linux

Odporúčania:
Odporúčame aktualizáciu na verziu 90.0.4430.93 pre Windows, Mac a Linux.

Zdroje:
https://chromereleases.googleblog.com/2021
https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_14.html
https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_20.html
https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_26.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci apríl nebola opravená žiadna kritická ani závažná zraniteľnosť v produkte Adobe Acrobat a Reader. Adobe prestal vydávať záplaty pre Flash Player 31. decembra 2020, teda nie je bezpečné ho používať.

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

5. Frameworky

Microsoft .NET Framework

V mesiaci apríl 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 apríl plánovanú štvrťročnú veľkú sadu aktualizácií. V Oracle Java SE boli dokopy opravené 4 zraniteľnosti, z čoho 2 sú závažné. Všetky tieto zraniteľnosti môžu byť vzdialene zneužité bez autentifikácie.

Zraniteľné systémy:
Oracle GraalVM Enterprise Edition: 19.3.5, 20.3.1.2, 21.0.0.2
Java SE: 7u291, 8u281, 11.0.10, 16
Java SE Embedded: 8u281

Odporúčania:
Odporúčame aktualizovať zraniteľné verzie Oracle GraalVM Enterprise Edition, Java SE a Java SE Embedded 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/cpuapr2021.html#AppendixJAVA

6. Iné závažné zraniteľnosti

Nové kritické zraniteľnosti emailového serveru Microsoft Exchange

Národná bezpečnostná agentúra (NSA) informovala spoločnosť Microsoft o objave kritických zraniteľností umožňujúcich vzdialene vykonať kód (RCE) v produkte Microsoft Exchange Server. Spoločnosť Microsoft vydala bezpečnostné aktualizácie a apeluje na administrátorov, aby urgentne aktualizovali emailové servery Microsoft Exchange vo svojej správe. Aktuálne nebolo zaznamenané zneužitie týchto zraniteľností, avšak Microsoft predpokladá, že je to len otázkou času. Viac informácií na stránke.

BleedingTooth – zraniteľnosti bluetooth v systéme Linux teraz už aj s exploitom

BleedingTooth je sada zraniteľností zariadení Bluetooth v operačnom systéme Linux. Zraniteľnosti umožňujú útočníkovi bez interakcie obete napadnúť zariadenia s oprávneniami jadra systému. Tieto staršie zraniteľnosti predstavujú stále riziko pre veľký počet neaktualizovaných zariadení po celom svete. Ešte väčšiu váhu im dáva aktuálne dostupná ukážka zneužitia zraniteľnosti (PoC exploit). Viac informácií na stránke.

Spoločnosť Cisco neopraví kritické zraniteľnosti svojich produktov

Spoločnosť Cisco sa rozhodla neopraviť kritické zraniteľnosti niektorých svojich smerovačov a zariadení firewall, ktorým skončila softvérová podpora. Spoločnosť Cisco vyzýva spoločnosti, ktoré tieto zariadenia používajú, aby zariadenia vymenili za novšie, podporované. Viac informácií na stránke.

Spoločnosť Cisco opravila kritickú zraniteľnosť produktu SD-WAN vManage

Spoločnosť Cisco vydala aktualizácie na opravu zraniteľností. Jedna zraniteľnosť získala hodnotenie „kritická“. Spoločnosť Cisco apeluje na administrátorov k čo najrýchlejšej oprave zariadení v ich správe. Viac informácií na stránke.

Stará zraniteľnosť firewallov od Spoločnosti Fortinet je aktívne zneužívaná

Stará zraniteľnosť firewallov Fortinet SSL VPN z roku 2018 je aktuálne aktívne zneužívaná. Okrem priamych zneužití zraniteľností, začali zraniteľnosť CVE-2018-13379 útočníci zneužívať aj na šírenie ransomvéru (napríklad ransomvér Cring). Rovnako s rozšírením povedomia o zneužiteľnosti zraniteľnosti a s poznatkom, že existuje množstvo zariadení, ktoré neboli administrátormi opravené, bolo pozorované aj masívne skenovanie sietí vyhľadávajúc zraniteľné zariadenia na ktoré by mohli útočníci potencionálne útočiť. Viac informácií na stránke.

V Pulse Connect Secure (PCS) SSL VPN bola opravená kritická aktívne zneužívaná zero-day zraniteľnosť

V Pulse Connect Secure (PCS) SSL VPN bola objavená a opravená aktívne zneužívaná zero-day zraniteľnosť, ktorej zneužitím môže dôjsť k vzdialenému vykonaniu kódu neautentifikovaným útočníkom. Zraniteľnosť dosahuje CVSS skóre 10. Viac informácií na stránke.

Spoločnosť SonicWall opravila kritické zraniteľnosti produktu pre emailovú bezpečnosť

Spoločnosť SonicWall opravila 3 vážne zraniteľnosti, ktoré získali hodnotenie CVSS 6,7 a 9,4. Najzávažnejšia zo zraniteľností by mohla útočníkovi umožniť vzdialene vytvoriť administrátorský účet poslaním špeciálne vytvorenej http požiadavky zraniteľnému zariadeniu. CSIRT.SK odporúča bezodkladne aktualizovať zraniteľné zariadenia vo svojej správe a predísť tak odcudzeniu dát, či možnému rozšíreniu malvéru v organizácii. Viac informácií na stránke.