Mesačný prehľad kritických zraniteľností
august 2020

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci august 10 kritických a 77 závažných zraniteľností.

Opravených bolo 5 kritických zraniteľností vedúcich ku poškodeniu pamäte. Zraniteľnosti CVE-2020-1477, CVE-2020-1492 a CVE-2020-1379, CVE-2020-1554 a CVE-2020-1525 existujú kvôli nesprávnemu narábaniu s objektmi v pamäti v programe Windows Media Foundation. Po ich zneužití môže útočník inštalovať programy, prezerať, mazať a meniť dáta.

Zraniteľnosť CVE-2020-1472 vzniká, ak používateľ vytvorí zraniteľné pripojenie zabezpečeného kanála Netlogon k radiču domény pomocou protokolu Netlogon Remote Protocol (MS-NRPC) a môže umožniť ľubovoľné navyšovanie privilégií používateľa. Útočník, ktorý úspešne zneužije túto chybu, by mohol spustiť vlastnú aplikáciu na zariadení v sieti.

Kritická zraniteľnosť CVE-2020-1374 vzniká, keď sa používateľ cez klientsky prístup k vzdialenej pracovnej ploche pripojí ku škodlivému serveru. Útočník po zneužití tejto zraniteľnosti môže spustiť ľubovoľný kód na počítači pripojeného používateľa.

Opravená kritická zraniteľnosť CVE-2020-1339 a CVE-2020-1435 súvisia s nesprávnym spracúvaním objektov v pamäti nástrojom Windows Media Audio Codec. Útočník po zneužití tejto zraniteľnosti môže prevziať kontrolu nad systémom.

Opravené kritické zraniteľnosti CVE-2020-1560, CVE-2020-1585 a CVE-2020-1574 vznikajú pri nesprávnom spracúvaní objektov v pamäti nástrojom Microsoft Windows Codecs Library. Útočník, ktorý úspešne zneužije tieto zraniteľnosti, by mohol vykonať ľubovoľný kód v danom systéme.

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 1709 for 32-bit Systems
Windows 10 Version 1709 for ARM64-based Systems
Windows 10 Version 1709 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 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)

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-2020-1339
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1379
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1477
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1492
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1525

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1554
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1560
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1574
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1585

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci august 1 kritickú a 19 závažných zraniteľností.

Opravená bola kritická zraniteľnosť CVE-2020-1483 existujúca v programe Microsoft Outlook, ktorý nedokáže správne spracovať objekty v pamäti. Útočník, ktorý úspešne zneužije túto chybu, by mohol vykonať ľubovoľný kód v kontexte aktuálneho používateľa. Ďalej môže útočník inštalovať programy, prezerať, mazať a meniť dáta.

Zraniteľné systémy:
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
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)

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-2020-1483

3. Internetové prehliadače

Microsoft Internet Explorer

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

Opravená bola kritická zraniteľnosť CVE-2020-1567, ktorá sa nachádza v spôsobe, akým nástroj MSHTML spracúva objekty v pamäti. Po jej zneužití môže útočník inštalovať programy, prezerať, mazať a meniť dáta alebo si vytvoriť nové účty s plnými užívateľskými právami.

Opravené boli aj kritické zraniteľnosti CVE-2020-1570 a CVE-2020-1380. Zraniteľnosti umožňujú vykonávanie vzdialeného kódu a vznikajú v spôsobe, akým skriptovací modul spracováva objekty v pamäti v programe Internet Explorer. Po jej zneužití môže útočník inštalovať programy, prezerať, mazať a meniť dáta a vykonávať inú aktivitu v kontexte aktuálneho používateľa.

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-2020-1380
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1567
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1570

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac v prehliadači Microsoft Edge 2 kritické a 1 závažnú zraniteľnosť.

Opravené kritické zraniteľnosti vznikajú v produktoch Microsoft Edge PDF Reader a v prehliadači Microsoft Edge kvôli nesprávnemu spracovaniu objektov v pamäti a ich zneužitie môže viesť k umožneniu vykonania vzdialeného kódu v prehliadači obete.

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-2020-1555
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1568

Mozilla Firefox

V mesiaci august bola opravená 1 kritická zraniteľnosť v prehliadači Firefox pre Android 68.10.1 a to CVE-2020-15647 umožňujúca čítanie súborov prehliadača vzdialeným webovým stránkam, čo viedlo k odhaleniu citlivých údajov vrátane súborov cookies.

V najnovšej verzii Firefox boli opravené 4 závažné zraniteľnosti. V najnovšej verzii Firefox ESR boli takisto opravené 3 závažné zraniteľnosti. Väčšina týchto zraniteľností sa týkala chýb umožňujúcich únik údajov z týchto prehliadačov.

Zraniteľné systémy:
Mozilla Firefox verzie staršie ako 80
Mozilla Firefox ESR verzie staršie ako 68.12

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 80 resp. Firefox ESR na 68.12.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-36/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-37/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-38/

Google Chrome

V mesiaci august bola vydaná oprava 15 závažných zraniteľností. Nebola opravená žiadna kritická zraniteľnosť.

Väčšina z opravených závažných zraniteľností vzniká pri použití odalokovaného miesta v pamäti a pri umožnení čítaní mimo hraníc.

Zraniteľné systémy:
Google Chrome verzie staršie ako 84.0.4147.125

Odporúčania:
Odporúčame aktualizáciu na verziu 84.0.4147.125

Zdroje:
https://chromereleases.googleblog.com/2020
https://chromereleases.googleblog.com/2020/08/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2020/08/stable-channel-update-for-desktop_18.html
https://chromereleases.googleblog.com/2020/08/stable-channel-update-for-desktop_25.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci august bolo v Adobe Acrobat a Reader opravených 5 kritických zraniteľností. Spoločnosť Adobe nevydala opravu žiadnych kritických zraniteľností pre Adobe Flash Player.

Väčšina opravených kritických zraniteľností súvisí s použitím odalokovaného miesta v pamäti a jej zneužitie môže viesť ku vzdialenému vykonaniu kódu.

Zraniteľné systémy:
Acrobat DC
Acrobat Reader DC
Acrobat 2020
Acrobat Reader 2020
Acrobat 2017
Acrobat Reader 2017
Acrobat 2015
Acrobat Reader 2015

Odporúčania:

Odporúčame aktualizáciu:
Acrobat DC na verziu 2020.012.20041
Acrobat Reader DC na verziu 2020.012.20041
Acrobat 2020 na verziu 2020.001.30005
Acrobat Reader 2020 na verziu 2020.001.30005
Acrobat 2017 na verziu 2017.011.30175
Acrobat Reader 2017 na verziu 2017.011.30175
Acrobat 2015 na verziu 2015.006.30527
Acrobat Reader 2015 na verziu 2015.006.30527

Zdroje:

https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/acrobat/apsb20-48.html

5. Frameworky

Microsoft .NET Framework

V mesiaci august 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 20. októbra 2020.

Zdroje:

https://www.oracle.com/technetwork/topics/security/alerts-086861.html
https://www.oracle.com/security-alerts/cpujul2020.html#AppendixJAVA

6. Iné závažné zraniteľnosti

Zraniteľnosť v softvéri Cisco ASA a FTD firewall umožňuje čítať súbory servera

Kvôli nedostatočnej validácii URL adresy z HTTP požiadaviek v produkte Cisco ASA a FTD firewall môže útočník vložiť do požiadavky cestu súborového systému servera. Vďaka tomu môže pristúpiť k dátam ktoré nie sú určené pre používateľov. Viac informácií na stránke.

Kritická zraniteľnosť v komponentoch .NET, SharePoint a Visual Studio umožňuje deserializáciu akéhokoľvek kódu

Opravená kritická zraniteľnosť sa nachádza v .NET Framework a produktoch SharePoint a Visual Studio. Prejavuje sa tým, že komponenty .NET slúžiace na prácu s datasetmi neskontrolujú zdrojový markup spracovaného XML súboru. Vďaka tomu útočník môže .NET aplikácii poslať XML súbor obsahujúci kód ktorý aplikácia vykoná. Viac informácií na stránke.

Zraniteľnosť zavádzača GRUB2 ohrozuje väčšinu Windows a Linux systémov

Spoločnosť Eclypsium objavila závažnú zraniteľnosť v zavádzači GRUB2, ktorá umožňuje vložiť do kódu zavádzača malvér, obísť mechanizmus Secure boot a získať perzistenciu aj v prípade reinštalácie operačného systému. Viac informácií na stránke.

Kritická zraniteľnosť v aplikácii vBulletin umožňuje vzdialené vykonávanie kódu bez autentifikácie

Zraniteľnosť v aplikácii vBulletin je spôsobená nedostatočnou kontrolou používateľských vstupov a viaže sa na nedostatočnú záplatu staršej zraniteľnosti. Na zneužitie je potrebné poslať príkaz na renderovanie vlastnej šablóny s PHP konfiguračným kódom ktorý sa vykoná. Aplikácia vykoná príkaz aj bez autentifikácie. Viac informácií na stránke.

Zraniteľnosť v aplikácii TeamViewer umožňuje útočníkovi pripojiť sa bez znalosti hesla

Nedostatočná kontrola vstupných parametrov URI schém aplikácie TeamViewer môže spôsobiť, že parametre sa vykonajú ako príkazy. Útočník tak môže podsunúť obeti vstup, ktorý spustí TeamViewer a vykoná požadovanú akciu. To je možné využiť na vytvorenie zdieľaného priečinka zo strany obete, vďaka čomu sa útočník nemusí autentifikovať. Viac informácií na stránke.

Microsoft vydal núdzový update pre Windows 8.1 a Server 2012 R2 kvôli kritickým zraniteľnostiam

Obe kritické zraniteľnosti sa nachádzajú v službe Remote Access Service a umožňujú zvýšenie oprávnení vzdialenému útočníkovi v prípade, že už má do systému prístup so schopnosťou spúšťania programov. Viac informácií na stránke.