Mesačný prehľad kritických zraniteľností júl 2020

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci júl 13 kritických a 81 závažných zraniteľností.

Opravených bolo 12 kritických zraniteľností umožňujúcich vzdialené vykonávanie kódu. Zraniteľnosti CVE-2020-1032, CVE-2020-1036 a CVE-2020-1040 - CVE-2020-1043 sa vyskytujú v produkte Hyper-V RemoteFX vGPU kvôli nesprávnemu overeniu vstupu autentifikovaného používateľa v hosťujúcom operačnom systéme.

Zraniteľnosť CVE-2020-1350 vzniká pri nesprávnom spracovaní požiadavky vo Windows DNS serveroch. Po jej zneužití môže útočník vykonať ľubovoľný kód v kontexte účtu lokálneho systému.

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.

Opravené kritické zraniteľnosti CVE-2020-1409 a CVE-2020-1435 vznikajú pri nesprávnom spracúvaní objektov v pamäti nástrojmi DirectWrite a Graphics Device Interface. Útočník po zneužití týchto zraniteľností môže prevziať kontrolu nad systémom.

Opravená kritická zraniteľnosť CVE-2020-1421 vzniká pri spracovaní .LNK súborov. Po otvorení súboru aktuálnym používateľom je pri otvorení súboru s touto príponou spustený škodlivý kód, ktorý môže vykonávať ľubovoľné príkazy v závislosti od kontextu aktuálneho používateľa.

Kritická zraniteľnosť CVE-2020-1410 vzniká keď Windows Address Book (WAB) nedokáže správne spracovať súbory vizitiek. Na umožnenie zneužitia tejto zraniteľnosti by používateľ musel otvoriť špeciálne vytvorenú vizitku.

Posledná opravená kritická zraniteľnosť CVE-2020-1436 vzniká keď knižnica písiem Windows nesprávne zaobchádza so špeciálne vytvorenými fontmi. Po jej zneužití môže útočník inštalovať programy, prezerať, mazať a meniť dáta.

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-2020-1032
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1036
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1040
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1041
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1042
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1043
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1374
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1409
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1410
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1421
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1435
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1436

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci júl 4 kritické a 17 závažných zraniteľností.

Opravená bola kritická zraniteľnosť CVE-2020-1025 umožňujúca neoprávnené navýšenie oprávnení pre používateľa. Táto zraniteľnosť vzniká kvôli nesprávnemu overovaniu tokenov protokolu OAuth na Microsoft SharePoint a Skype for Business serveroch.

Ďalšia kritická zraniteľnosť CVE-2020-1147 vzniká takisto v službe Microsoft SharePoint, v .NET framework-u a v nástroji Visual Studio pri zlyhaní overovania pôvodu XML vstupu. Útočník, ktorý úspešne zneužil túto zraniteľnosť, by mohol spustiť ľubovoľný kód v kontexte procesu zodpovedného za deserializáciu obsahu XML vstupu.

Opravená bola kritická zraniteľnosť CVE-2020-1349, ktorá vzniká keď Microsoft Outlook nedokáže správne spracovať objekty v pamäti. Útočník, ktorý by úspešne zneužil túto chybu zabezpečenia, by mohol použiť špeciálne vytvorený súbor na vykonávanie akcií v kontexte zabezpečenia aktuálneho používateľa.

Poslednou opravenou zraniteľnosťou za tento mesiac bola CVE-2020-1439 v softvéri PerformancePoint Services pre SharePoint server, ktorá vzniká pri zlyhaní overovania pôvodu XML vstupu.

Zraniteľné systémy:
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Lync Server 2013
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)
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2010 Service Pack 2
Microsoft SharePoint Server 2010 Service Pack 2
Microsoft SharePoint Server 2019
Microsoft SharePoint Server 2019
Microsoft SharePoint Server 2019
Microsoft SharePoint Server 2019
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
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1025
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1147
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1349
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1439

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft opravila tento mesiac v prehliadači Internet Explorer 1 kritickú zraniteľnosť.

Opravená bola kritická zraniteľnosť CVE-2020-1403, ktorá sa nachádza v spôsobe akým modul VBScript spracúva objekty v pamäti. Po jej zneužití môže útočník inštalovať programy, prezerať, mazať a meniť dáta, alebo si vytvoriť nové účty s plnými používateľskými právami.

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-2020-1403

Microsoft Edge

Spoločnosť Microsoft neopravila tento mesiac v prehliadači Microsoft Edge žiadne kritické, no opravila 2 závažné zraniteľnosti.

Opravené závažné zraniteľnosti vznikajú v produktoch Microsoft Edge PDF Reader a Skype for Business pre Microsoft Edge a ich zneužitie môže viesť k úniku údajov z prehliadača.

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-2020-1433
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1462

Mozilla Firefox

V mesiaci júl 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 a Firefox ESR boli opravené 4 závažné zraniteľnosti. Väčšina týchto zraniteľností sa týkala chýb umožňujúcich únik údajov z týchto prehliadačov.

Zraniteľné systémy:
Mozilla Firefox pre Android verzie staršie ako 68.11.0
Mozilla Firefox verzie staršie ako 79.0
Mozilla Firefox ESR verzie staršie ako 68.11.0

Odporúčania:
Odporúčame aktualizáciu Firefox pre Android na verziu 68.11.0 resp. Firefox na verziu 79.0 resp. Firefox ESR na 68.11.0.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-27/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-30/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-31/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-32/

Google Chrome

V mesiaci júl bola vydaná oprava na 1 kritickú a 12 závažných zraniteľností.

Kritická zraniteľnosť CVE-2020-6510 vzniká pri pretečení vyrovnávacej pamäte haldy pri načítaní na pozadí. Väčšina z opravených závažných zraniteľností vzniká pri použití odalokovaného miesta v pamäti.

Zraniteľné systémy:
Google Chrome verzie staršie ako 84.0.4147.105

Odporúčania:
Odporúčame aktualizáciu na verziu 84.0.4147.105

Zdroje:
https://chromereleases.googleblog.com/2020
https://chromereleases.googleblog.com/2020/07/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2020/07/stable-channel-update-for-desktop_27.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci júl spoločnosť Adobe nevydala žiadne opravy pre zraniteľnosti v produktoch Adobe Flash Player ani Adobe Acrobat a Reader.

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

5. Frameworky

Microsoft .NET Framework

V mesiaci júl vydala spoločnosť Microsoft opravnú aktualizáciu pre 1 kritickú zraniteľnosť v produkte .NET Framework.

Kritická zraniteľnosť CVE-2020-1147 vzniká v Microsoft SharePoint, v .NET framework-u a v nástroji Visual Studio pri zlyhaní overovania pôvodu XML vstupu. Útočník, ktorý úspešne zneužil túto zraniteľnosť, môže vykonať ľubovoľný kód v kontexte procesu zodpovedného za deserializáciu obsahu XML vstupu.

Zraniteľné systémy:
.NET Core 2.1 verzie staršie ako 2.1.20
.NET Core 3.1 verzie staršie ako 3.1.6

Odporúčania:
Odporúčame aktualizáciu .NET Core 2.1 na verziu 2.1.20 resp. .NET Core 3.1 na verziu 3.1.6

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1147

Oracle Java

Spoločnosť Oracle vydala v mesiaci júl plánovanú štvrťročnú veľkú sadu aktualizácií. V produktoch Java SE a Java SE Embedded bolo celkovo opravených 11 zraniteľností. Najzávažnejšie z nich sa nachádzajú v komponentoch JavaFX, 2D, ImageIO a v knižniciach produktov Java SE a Java SE Embedded.

Zraniteľné systémy:
Java SE: 7u261, 8u251, 11.0.7, 14.0.1
Java SE Embedded: 8u251

Odporúčania:
Odporúčame aktualizovať zraniteľné verzie 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/technetwork/topics/security/alerts-086861.html
https://www.oracle.com/security-alerts/cpujul2020.html#AppendixJAVA

6. Iné závažné zraniteľnosti

Kritická zraniteľnosť v produktoch F5

Spoločnosť F5 vydala bezpečnostné aktualizácie, ktoré opravujú kritickú bezpečnostnú zraniteľnosť produktov BIG-IP s hodnotou CVSS skóre 10. Túto zraniteľnosť môže zneužiť útočník na celkovú kompromitáciu informačného systému ku ktorému má zraniteľné zariadenie prístup. Viac informácií na stránke.

Dve kritické zraniteľnosti vo virtuálnom grafickom rozhraní produktov VMware

Spoločnosť VMware vydala bezpečnostné aktualizácie na opravu viacerých zraniteľností v programoch VMware ESXi, Workstation a Fusion. Dve najzávažnejšie z nich umožňujú vykonávať kód na hypervízorovi z virtuálneho zariadenia. Viac informácií na stránke.

Kritické zraniteľnosti v TCP/IP knižnici pre zariadenia IoT

Bezpečnostná výskumná skupina JSOF objavila 19 zraniteľností v knižnici spoločnosti Treck protokolov TCP/IP využívanú vyše 20 rokov v IoT zariadeniach, ktoré nazvala Ripple20. 5 z 19 je klasifikovaných podľa CVSS skóre ako „High“, ostatné „Medium“ alebo „Low“. Chyby sa týkajú protokolov IPv4, IPv6, UDP, DNS, DHCP, TCP, ICMPv4 a ARP. Viac informácií na stránke.

V systéme Palo Alto PAN-OS bola objavená kritická bezpečnostná zraniteľnosť

V protokole SAML sa nachádza kritická zraniteľnosť. Táto chyba sa nachádza v kontrolných mechanizmoch autentifikácie. Nesprávne overovanie podpisov v protokole SAML systému PAN-OS, umožňuje neoverenému útočníkovi v sieti pristupovať ku chráneným zdrojom. Aby mohol útočník zraniteľnosť zneužiť, musí získať sieťový prístup na postihnutý server. Viac informácií na stránke.

Kritická zraniteľnosť v produktoch SAP

Spoločnosť Onapsis v máji objavila a ohlásila kritickú zraniteľnosť v produktoch spoločnosti SAP (CVSS 10). Spoločnosť SAP vydala záplatu na kritickú zraniteľnosť, ktorá sa nachádza v jej komponente NetWeaver. Zraniteľnosť umožňuje neautentifikovanému útočníkovi vytvárať účty s najvyššími oprávneniami a vykonávať systémové príkazy, teda úplne kompromitovať systémy využívajúce zraniteľné produkty SAP, pristupovať k citlivým údajom a zasahovať do operácií spoločnosti. Viac informácií na stránke.

SIGRed - kritická zraniteľnosť Windows DNS serverov

Spoločnosť Microsoft opravila kritickú zraniteľnosť DNS (CVSS 10), ktorá je vo všetkých Windows serveroch konfigurovaných ako DNS už 17 rokov. Útočníkovi umožňuje preposielať citlivé dáta na svoj server, manipulovať so sieťovým prenosom, a tiež kompromitovať celú sieť. Viac informácií na stránke.

Kritické zraniteľnosti v produktoch spoločnosti Adobe

Spoločnosť Adobe vydala záplatu opravujúcu kritické zraniteľnosti vo svojich produktoch Photoshop, Bridge a Prelude. 12 kritických zraniteľností vo verziách produktov pre Windows je spôsobených možnosťou čítať a zapisovať mimo hraníc, čo môže viesť k vykonaniu ľubovoľného kódu. Viac informácií na stránke.

Chyba vo funkcii Vanity URL aplikácie Zoom umožňuje vydávať sa za používateľa tejto funkcie

Funkcia Vanity URL v aplikácii Zoom slúžiaca na vytvorenie vlastnej URL nie je chránená proti impersonácii. K pozvánke na stretnutie je možné uviesť akúkoľvek subdoménu, vďaka čomu môže vyzerať rovnako ako pozvánka od spoločnosti, ktorá túto doménu používa. Spoločnosť Zoom Video Communications vydala na túto chybu záplatu. Viac informácií na stránke.