Mesačný prehľad kritických zraniteľností jún 2020

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci jún 6 kritických a 92 závažných zraniteľností.

Opravených bolo 6 kritických zraniteľností umožňujúcich vzdialené vykonávanie kódu. Zraniteľnosť CVE-2020-1248 sa vyskytuje spôsobe, akým súčasti Microsoft Graphics Device Interface spracúvajú objekty v pamäti.

Zraniteľnosť CVE-2020-1281 vzniká pri nesprávnom spracovaní užívateľského vstupu v Microsoft Windows OLE. Po jej zneužití môže útočník inštalovať programy, prezerať, mazať a meniť dáta.

Ďalšia kritická zraniteľnosť CVE-2020-1286 vzniká keď Windows Shell nedostatočne overuje cesty k súborom. Útočník po zneužití tejto zraniteľnosti môže spustiť ľubovoľný kód v kontexte aktuálneho používateľa. Útočník tak môže inštalovať programy, prezerať, mazať a meniť dáta.

Opravená kritická zraniteľnosť CVE-2020-1299 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-2020-1300 vzniká keď Microsoft Windows nedokáže spracovať súbory kabinetu. Na umožnenie zneužitia tejto zraniteľnosti by používateľ musel otvoriť špeciálne vytvorený súbor alebo nainštalovať škodlivý súbor kabinetu maskovaný ako ovládač tlačiarne.

Opravená bola kritická zraniteľnosť CVE-2020-1425, vznikajúca keď knižnica Microsoft Windows Codecs Library nesprávne spracúva objekty v pamäti. Útočník, ktorý by úspešne zneužil túto chybu, by mohol získať informácie na ďalšie ohrozenie systému používateľa.

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 1803 (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-2020-1248

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1281
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1286
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1299
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1300
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1425

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci jún 1 kritickú a 18 závažných zraniteľností.

Opravená bola kritická zraniteľnosť CVE-2020-1181 umožňujúca vzdialené vykonávanie kódu. Zraniteľnosť vzniká na Microsoft SharePoint Server, keď sa nepodarí správne identifikovať a filtrovať nebezpečné webové ovládače ASP.Net. Autentifikovaný útočník, ktorý úspešne zneužil túto chybu zabezpečenia, by mohol použiť špeciálne vytvorenú stránku na vykonávanie akcií v kontexte zabezpečenia procesu zdieľania aplikácií SharePoint.

Zraniteľné systémy:
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Foundation 2010 Service Pack 2
Microsoft SharePoint Foundation 2013 Service Pack 1

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-2020-1181

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft opravila tento mesiac v prehliadači Internet Explorer 4 kritické zraniteľnosti.

Opravené boli kritické zraniteľnosť CVE-2020-1231, CVE-2020-1216 a CVE-2020-1260 vznikajúce pri chybnom spracúvaní objektov v pamäti modulom VBScript. Tieto zraniteľnosti

by mohli poškodiť pamäť takým spôsobom, že by útočník mohol vykonať ľubovoľný kód v kontexte aktuálneho používateľa. Kritická zraniteľnosť CVE-2020-1219 vzniká v spôsobe, akým prehliadače Microsoft pristupujú k objektom v pamäti. Po jej zneužití môže útočník inštalovať programy, prezerať, mazať a meniť dáta alebo si vytvoriť nové účty s plnými užívateľskými 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-2020-1213
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1216
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1219
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1260

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac v prehliadači Microsoft Edge 2 kritické zraniteľnosti.

Obe opravené zraniteľnosti sa týkajú poškodenia pamäte. Kritická zraniteľnosť CVE-2020-1073 vzniká v spôsobe, akým skriptovací stroj ChakraCore spracúva objekty v pamäti. Táto zraniteľnosť by mohla poškodiť pamäť takým spôsobom, že by útočník mohol vykonať ľubovoľný kód v kontexte aktuálneho používateľa.

Kritická zraniteľnosť CVE-2020-1219 vzniká keď prehliadač Microsoft pristupuje k objektom v pamäti. Po jej zneužití môže útočník inštalovať programy, prezerať, mazať a meniť dáta alebo si vytvoriť nové účty s plnými užívateľskými právami.

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-2020-1073
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1219

Mozilla Firefox

V mesiaci neboli opravené žiadne kritické zraniteľnosti. V najnovšej verzii Firefox bolo opravených 8 závažných zraniteľností. V najnovšej verzii Firefox ESR bolo opravených 5 závažných zraniteľností. Väčšina týchto zraniteľností sa týkala použitia odalokovaného miesta v pamäti.

Zraniteľné systémy:
Mozilla Firefox verzie staršie ako 78
Mozilla Firefox ESR verzie staršie ako 68.10

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 78.0.1 resp. Firefox ESR na 68.10.1.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-20/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-21/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-22/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-23/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-24/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-25/

Google Chrome

V mesiaci jún bola vydaná oprava 8 závažných zraniteľností.

Závažné zraniteľnosti CVE-2020-6509, CVE-2020-6505, CVE-2020-6493 a CVE-2020-6496 sa súvisia s použitím odalokovaného miesta v pamäti. Zvyšné 4 opravené zraniteľnosti súvisia s nedostatočným nastavením politík a zápisom mimo hraníc v nástroji V8.

Zraniteľné systémy:
Google Chrome verzie staršie ako 83.0.4103.116

Odporúčania:
Odporúčame aktualizáciu na verziu 83.0.4103.116

Zdroje:
https://chromereleases.googleblog.com/2020
https://chromereleases.googleblog.com/2020/06/stable-channel-update-for-desktop_15.html
https://chromereleases.googleblog.com/2020/06/stable-channel-update-for-desktop_22.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci jún bola v Adobe Flash Player opravená 1 kritická zraniteľnosť. Spoločnosť Adobe nevydala opravu žiadnych kritických zraniteľností pre Adobe Acrobat a Reader.

Opravená kritická zraniteľnosť CVE-2020-9633 súvisí s použitím odalokovaného miesta v pamäti a jej zneužitie môže viesť k vykonaniu ľubovoľného kódu.

Zraniteľné systémy:
Adobe Flash Player Desktop Runtime
Adobe Flash Player for Google Chrome
Adobe Flash Player for Microsoft Edge and Internet Explorer 11

Odporúčania:
Odporúčame aktualizáciu:
Adobe Flash Player Desktop Runtime na verziu 32.0.0.387
Adobe Flash Player for Google Chrome na verziu 32.0.0.387
Adobe Flash Player for Microsoft Edge and Internet Explorer 11 na verziu 32.0.0.387

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/flash-player/apsb20-30.html

5. Frameworky

Microsoft .NET Framework

V mesiaci jún nevydala spoločnosť Microsoft žiadne opravné aktualizácie pre .NET Framework.

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

Oracle Java

Veľká sada opráv je plánovaná na 14. júla 2020.

Zdroje:
https://www.oracle.com/technetwork/topics/security/alerts-086861.html

6. Iné závažné zraniteľnosti

Kritické zraniteľnosti v zariadeniach Cisco IOS / IOS XE

Spoločnosť Cisco oznámila, že opravila 25 kritických a závažných zraniteľností v routeroch využívajúcich operačný systém Cisco IOS / IOS XE. Tri najkritickejšie umožňujú obídenie autentifikácie, vykonávanie príkazov či vykonanie DoS útokov. Viac informácií na stránke.

Zraniteľnosť v systéme Cisco NX-OS

V operačnom systéme sieťových prvkov NX-OS od spoločnosti Cisco bola nájdená zraniteľnosť, ktorá umožňuje obchádzať pravidlá konfigurované v zozname ACL, čo umožňuje kompromitáciu siete, alebo vykonanie DoS útoku. Útočník tiež získa možnosť preposielať svoje škodlivé pakety cez zraniteľné zariadenia a vykonávať tak DDoS útoky, či získavať informácie o ďalších obetiach. Viac informácií na stránke.

Zraniteľnosť SMBleed protokolu Windows Server Message Block (SMBv3)

Spoločnosť ZecOps odhalila novú kritickú bezpečnostnú zraniteľnosť v dekompresnej funkcii SMBv3.1.1, v ktorej boli nedávno objavené aj zraniteľnosti SMBGhost a EternalDarkness.

Zraniteľnosť dovoľuje únik citlivých dát, ktoré môžu byť ďalej zneužité na vzdialené vykonávanie kódu a kompromitáciu zraniteľného systému. Viac informácií na stránke.