Mesačný prehľad kritických zraniteľností
október 2020

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci október 7 kritických a 47 závažných zraniteľností.

Šesť z týchto kritických zraniteľností umožňuje vzdialené vykonávanie ľubovoľného kódu útočníkom. Zraniteľnosť CVE-2020-16891 umožňujúca vzdialené vykonávanie kódu súvisí s tým, že Windows Hyper-V nesprávne overuje vstup od autentifikovaného používateľa. Útočník by túto chybu mohol zneužiť na vykonanie ľubovoľného kódu na hostiteľskom operačnom systéme.

Zraniteľnosť CVE-2020-16898 vzniká, ak zásobník TCP/IP systému Windows nesprávne spracúva pakety smerovača ICMPv6. Úspešným zneužitím tejto chyby útočník môže vykonávať ľubovoľný kód na cieľovom serveri alebo klientovi.

Opravená bola kritická zraniteľnosť CVE-2020-16911, ktorá tiež umožňuje vzdialené vykonávanie kódu. Existuje v spôsobe, akým rozhranie Windows Graphics Device Interface (GDI) narába s objektmi v pamäti. Útočník je zneužitím tejto chyby schopný prevziať plnú kontrolu nad systémom.

Zraniteľnosť CVE-2020-16915, ktorej zneužitím môže dôjsť k poškodeniu pamäte existuje, ak Windows Media Foundation nesprávne narába s objektmi v pamäti. Útočník je úspešným zneužitím tejto chyby schopný inštalovať programy, prezerať a meniť údaje, alebo vytvárať nové účty s administrátorskými oprávneniami.

Zraniteľnosť CVE-2020-16923 vzniká v prípade, že Microsoft Graphics Components nesprávne pracujú s objektmi v pamäti. Útočník zneužitím tejto chyby môže vykonávať ľubovoľný kód na cieľovom systéme.

Opravené boli aj zraniteľnosti CVE-2020-16967 a CVE-2020-16968, ktoré vznikajú, keď Windows Camera Codec Pack nesprávne narába s objektmi v pamäti. Útočník je vďaka úspešnému zneužitiu chyby schopný vykonávať ľubovoľný kód v kontexte aktuálne prihláseného užívateľa. Využitie týchto chýb zabezpečenia vyžaduje, aby používateľ otvoril špeciálne vytvorený súbor s ovplyvnenou verziou balíka Windows Camera Codec Pack.

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-2020-16891
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-16898
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-16911
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-16915
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-16923
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-16967
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-16968

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci október 4 kritické a 19 závažných zraniteľností.

Všetky štyri kritické zraniteľnosti umožňujú vzdialené vykonávanie kódu. Zraniteľnosť CVE-2020-16947 existuje v produkte Microsoft Outlook, keď nedokáže správne spracovať objekty v pamäti. Útočník je úspešným zneužitím tejto chyby schopný vykonávať ľubovoľný kód v kontexte aktuálne prihláseného používateľa.

Opravené boli zraniteľnosti CVE-2020-16951 a CVE-2020-16952 v Microsoft SharePoint, ktoré sa dajú zneužiť, keď softvér nedokáže skontrolovať zdrojové označenie balíka aplikácie. Útočník, ktorý úspešne zneužije túto chybu by mohol vykonávať ľubovoľný kód. Využitie tejto chyby zabezpečenia vyžaduje, aby používateľ nahral špeciálne vytvorený balík aplikácií SharePoint do zraniteľnej verzie SharePointu.

Poslednou kritickou zraniteľnosťou je CVE-2020-17003, ktorá sa dá zneužiť, keď vykresľovací modul Base3D nesprávne spracováva pamäť. Jej zneužitie tiež útočníkovi povoľuje vykonávať ľubovoľný kód.

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 2016 (32-bit edition)
Microsoft Outlook 2016 (64-bit edition)
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2019
3D Viewer

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-2020-16947
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-16951
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-16952
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17003

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft neopravila v mesiaci október v prehliadači Internet Explorer žiadnu kritickú ani závažnú zraniteľnosť.

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

Microsoft Edge

Spoločnosť Microsoft neopravila v mesiaci október v prehliadači Edge žiadnu kritickú ani závažnú zraniteľnosť.

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

Mozilla Firefox

V mesiaci október nebola opravená žiadna kritická zraniteľnosť pre Firefox ani Firefox ESR. V najnovšej verzii Firefox boli opravené 4 závažné zraniteľnosti a vo Firefox ESR 2 závažné zraniteľnosti. Zneužitie väčšiny z nich môže viesť k poškodeniu pamäte.

Zraniteľné systémy:
Mozilla Firefox verzie staršej ako 82
Mozilla Firefox ESR verzie staršej ako 78.4

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 82 resp. Firefox ESR na 78.4.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-45/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-46/

Google Chrome

V mesiaci október bola vydaná oprava 1 kritickej a 11 závažných zraniteľností. Väčšina z týchto zraniteľností súvisí s použitím odalokovaného miesta v pamäti, prípadne sa jedná o pretečenie celočíselnej premennej.

Zraniteľné systémy:
Google Chrome verzie staršie ako 86.0.4240.111

Odporúčania:
Odporúčame aktualizáciu na verziu 86.0.4240.111

Zdroje:
https://chromereleases.googleblog.com/2020
https://chromereleases.googleblog.com/2020/10/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2020/10/stable-channel-update-for-desktop_12.html
https://chromereleases.googleblog.com/2020/10/stable-channel-update-for-desktop_20.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci október nebola vydaná žiadna oprava pre Adobe Acrobat a Reader. Spoločnosť Adobe vydala opravu 1 kritickej zraniteľnosti pre Adobe Flash Player. Jedná sa o dereferenciu nulového ukazovateľa, ktorá môže viesť k vykonávaniu 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 32.0.0.445
Adobe Flash Player for Google Chrome na verziu 32.0.0.445
Adobe Flash Player for Microsoft Edge and Internet Explorer 11 na verziu 32.0.0.445
Adobe Flash Player Desktop Runtime na verziu 32.0.0.445

Zdroje:

https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/flash-player/apsb20-58.html

5. Frameworky

Microsoft .NET Framework

V mesiaci október spoločnosť Microsoft vydala opravnú aktualizáciu pre 1 závažnú zraniteľnosť vo frameworku Microsoft .NET. Zneužitie zraniteľnosti CVE-2020-1108 môže viesť k narušeniu dostupnosti služby. Vzniká, keď .NET Core alebo .NET Framework nesprávne spracováva webové požiadavky. Túto zraniteľnosť je možné zneužiť na diaľku bez autentifikácie.

Zraniteľné systémy:

Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.5, 3.5.1
Microsoft .NET Framework 4.5.2
Microsoft .NET Framework 4.6, 4.6.1, 4.6.2
Microsoft .NET Framework 4.7, 4.7.1, 4.7.2
Microsoft .NET Framework 4.8

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-2020-16937

Oracle Java

Spoločnosť Oracle vydala v mesiaci október plánovanú štvrťročnú veľkú sadu aktualizácií. V produktoch Java SE a Java SE Embedded bolo celkovo opravených 8 zraniteľností. Väčšina z nich sa nachádza v knižniciach produktov Java SE a Java SE Embedded.

Zraniteľné systémy:
Java SE: 7u271, 8u261, 11.0.8, 15
Java SE Embedded: 8u261

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/cpuoct2020.html#AppendixJava

6. Iné závažné zraniteľnosti

Cisco vydalo záplaty pre aktívne zneužívané DoS zraniteľnosti v IOS XR

Zraniteľnosti triedy DoS môže zneužiť neautentifikovaný útočník a vedú ku zlyhaniu IGMP procesu alebo vyčerpaniu operačnej pamäte. Zneužitie zraniteľností je možné, len ak sa používa multicast routing a zariadenie môže prijímať DVMPR prevádzku. Viac informácií na stránke.

Kritickú zraniteľnosť v Adobe Flash Player je možné využiť na vzdialené vykonávanie kódu

Zraniteľnosť je spôsobená dereferenciou nulového ukazovateľa a spôsobuje zlyhanie programu Adobe Flash Player. Je možné zneužiť ju aj na vykonanie kódu, ktorý je možné poslať aj vzdialene v HTTP odpovedi, ktorú Flash Player spracuje. Viac informácií na stránke.

VMware - kritické zraniteľnosti v ESXi, Workstation, Fusion a NSX-T

Spoločnosť VMware odstránila zraniteľnosti vyskytujúce sa v ESXi, Workstation, Fusion a NSX-T. Tieto chyby vo všeobecnosti môžu viesť k vzdialenému vykonávaniu kódu na zraniteľných zariadeniach. Útočníci tiež môžu získavať rôzne informácie, eskalovať oprávnenia, prípadne môže dôjsť k narušeniu

dostupnosti služby. Na serveri vCenter dochádza k chybe funkcie zabezpečenia pri aktualizácii. Útočník je teda schopný prevziať kontrolu nad spojením. Viac informácií na stránke.

Spoločnosť Google vydala záplatu na zero-day zraniteľnosť v prehliadači Chrome. Môže spôsobiť poškodenie pamäte.

Kvôli kritickej zero-day zraniteľnosti v prehliadači Chrome, konkrétne v knižnici FreeType, môže dôjsť k pretečeniu medzipamäte haldy, čo spôsobuje poškodenie pamäte zariadenia. Útočníci môžu chybu zneužiť na vykonávanie ľubovoľného kódu. Viac informácií na stránke.

NAS zariadenia od spoločnosti QNAP obsahujú 2 kritické zraniteľnosti

Obe kritické zraniteľnosti sa nachádzajú v aplikácii Helpdesk a sú spôsobené nesprávnou kontrolou prístupu. Vzdialený útočník môže zraniteľnosti zneužiť na získanie kontroly nad sieťovými úložnými zariadeniami (NAS). Viac informácií na stránke.