Mesačný prehľad kritických zraniteľností

September 2017

1. Operačné systémy Microsoft Windows

V septembri vydala spoločnosť Microsoft opravu kritickej zraniteľnosti CVE-2017-0161 v komponente NetBIOS, ktorá útočníkovi umožňuje na diaľku vykonať škodlivý kód zapríčinením chyby v súbehu viacerých vlákien prostredníctvom zaslania špeciálne pripravených NetBT Session paketov. Neúspešný pokus o zneužitie môže zapríčiniť zamedzenie dostupnosti napadnutého zariadenia.

Ďalšia vydaná oprava sa týka kritickej zraniteľnosti CVE-2017-8686 vo Windows DHCP Server, ktorá spočíva v spôsobení narušenia integrity pamäte prostredníctvom zaslania špeciálne pripravených paketov DHCP serveru, pracujúcom v režime "failover". V dôsledku úspešného zneužitia získa útočník možnosť vzdialeného vykonania škodlivého kódu, prípadne zamedzenie dostupnosti služby.

Kritická zraniteľnosť CVE-2017-8682 vo Win32k Graphics (súčasť Windows knižnice písiem) umožňuje útočníkovi na diaľku získať plnú kontrolu nad zariadením, a to zneužitím chyby pri narábaní s vloženými písmami. Používateľské účty s menšími právomocami môžu byť zasiahnuté menej. Pre úspešné zneužitie musí používateľ navštíviť špeciálne pripravenú webovú stránku, na ktorú musí útočník používateľa nalákať. Inou možnosťou zneužitia je otvorenie pripraveného škodlivého súboru, ktorý útočník rozoslal emailom. Exploit na túto zraniteľnosť je verejne dostupný.

V rámci septembrového balíka aktualizácií vydala spoločnosť Microsoft opravy zraniteľností CVE-2017-8680, CVE-2017-8681, CVE-2017-8684 a CVE-2017-8685 v komponente Windows GDI+, označených ako dôležité. Zraniteľnosť spočíva v možnosti pre lokálneho autentifikovaného útočníka spustiť špeciálne pripravenú aplikáciu a zapríčiniť únik adries z pamäťového priestoru kernelu. Tieto informácie je potenciálne možné zneužiť pri ďalšom pokračovaní útoku. Exploity na všetky štyri uvedené zraniteľnosti sú verejne dostupné.

V septembri vydané opravy zraniteľností CVE-2017-8678, CVE-2017-8708 a CVE-2017-8687 vo Windows kerneli sú tiež označené ako dôležité. Lokálny autentifikovaný útočník môže spustením špeciálne pripravenej aplikácie zneužiť chyby pri narábaní s pamäťou, prípadne jej inicializácii. Týmto môže útočník obísť randomizáciu kernelového adresového priestoru a získať informácie, ktoré môže ďalej zneužiť pri pokračovaní útoku. Exploity na tieto zraniteľnosti sú verejne dostupné.

Spoločnosť Microsoft opravila dôležitú zraniteľnosť CVE-2017-8683 v komponente Win32k Graphics. Lokálny autentifikovaný útočník môže spustením špeciálne pripravenej aplikácie spôsobiť únik informácií potenciálne zneužiteľných na pokračovanie útoku. Na túto zraniteľnosť je tiež verejne dostupný exploit.

Zraniteľné systémy:

Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows 8.1 for 32-bit Systems
Windows 8.1 for x64-based Systems
Windows RT 8.1
Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1511 for 32-bit Systems
Windows 10 Version 1511 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1703 for 32-bit Systems
Windows 10 Version 1703 for x64-based Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1

Windows Server 2012
Windows Server 2012 R2
Windows Server 2016

Odporúčania:

Vzhľadom na zvýšenú pravdepodobnosť zneužitia niektorých uvedených zraniteľností a existencie verejne dostupných exploitov, odporúčame čo najskôr 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-2017-0161
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8686
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8682
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8680
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8678
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8708
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8683

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft v rámci septembrového balíka aktualizácií vydala opravu kritickej zraniteľnosti CVE-2017-8682, týkajúcej sa aj aplikácií z balíka Microsoft Office, ako jedného z možných vektorov útoku. Podrobnosti k tejto zraniteľnosti, ako aj fakt o verejne dostupnom exploite, sú uvedené v predošlej kapitole.

Opravená kritická zraniteľnosť CVE-2017-8676 vo Windows GDI+ umožňuje lokálnemu autentifikovanému útočníkovi spôsobiť únik informácií, ktoré sú potenciálne zneužiteľné pri pokračovaní útoku, prostredníctvom spustenia špeciálne pripravenej aplikácie. Súvis z aplikáciami balíka Microsoft Office spočíva v možnosti zneužitia panelu náhľadu ako vektora útoku.

Ďalšou opravenou kritickou zraniteľnosťou je CVE-2017-8696 spočívajúca v chybe narábania s pamäťou v komponente Windows Uniscribe. Útočník môže úspešným zneužitím získať plnú kontrolu nad zariadením. Používateľské účty s nižšími právomocami môžu byť zasiahnuté menej. Pre úspešné zneužitie môže útočník pripraviť špeciálnu škodlivú webovú stránku a následne nalákať používateľa túto stránku navštíviť. Inou možnosťou pre útočníka je pripravenie škodlivého súboru, jeho dopravenie ku používateľovi, napr. prostredníctvom emailu alebo zdieľania obsahu, a následné nalákanie na jeho otvorenie.

Zraniteľné systémy:

Microsoft Office 2007 Service Pack 3
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office Web Apps 2010 Service Pack 2
Microsoft Office Word Viewer
Microsoft Office for Mac 2011
Microsoft Office 2016 for Mac
Microsoft Live Meeting 2007 Add-in
Microsoft Live Meeting 2007 Console
Microsoft Lync 2010
Microsoft Lync 2010 Attendee
Microsoft Lync 2013 Service Pack 1
Microsoft Lync Basic 2013 Service Pack 1
Skype for Business 2016
Skype for Business 2016 Basic

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-2017-8682
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8676
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8696

3. Internetové prehliadače

Microsoft Internet Explorer

V rámci septembrového balíka opráv boli spoločnosťou Microsoft vydané opravy kritických zraniteľností CVE-2017-8741 a CVE-2017-8748 v JavaScript engine, ktoré útočníkovi umožňujú spôsobiť narušenie integrity pamäte a následne vzdialene vykonať škodlivý kód s právomocami práve prihláseného používateľa. Pre úspešné zneužitie potrebuje útočník pripraviť špeciálnu webovú stránku, alebo škodlivý webový obsah a nalákať používateľa na navštívenie danej stránky. Druhou možnosťou je umiestnenie JavaScript obsahu do Microsoft Office dokumentu, ktorého otvorením rovnako dôjde ku zneužitiu zraniteľností.

Ďalšie vydané opravy kritických zraniteľností, CVE-2017-8747, CVE-2017-8749 a CVE-2017-8750, spočívajúcich v chybe v prístupe k objektom v pamäti. Úspešným zneužitím získa útočník možnosť vzdialeného vykonania škodlivého kódu s právomocami práve prihláseného používateľa. Pre úspešné zneužitie potrebuje útočník špeciálne pripravenú webovú stránku, prípadne stránku so zdieľaným používateľským obsahom, a následne nalákať používateľa na navštívenie danej stránky.

Zraniteľné systémy:
Microsoft Internet Explorer 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-2017-8741
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8747

Microsoft Edge

V rámci septembrového balíka aktualizácií boli vydané opravy 21 kritických zraniteľností.

V skriptovacom engine Chakra boli opravené zraniteľnosti CVE-2017-8729, CVE-2017-8738, CVE-2017-8752, CVE-2017-8753, CVE-2017-8756, CVE-2017-8740, CVE-2017-8755 a CVE-2017-11764, ktoré spočívajú v chybe pri narábaní s objektami v pamäti. To môže útočník zneužiť na spôsobenie narušenia integrity pamäte, čím získa možnosť na diaľku vykonať škodlivý kód s právomocami práve prihláseného používateľa. Útočník potrebuje vytvoriť škodlivú webstránku, prípadne umiestniť škodlivý obsah na stránku so zdieľaným používateľským obsahom. Pre úspešné zneužitie útočník potrebuje používateľa nalákať na návštevu pripravenej stránky, napríklad prostredníctvom emailovej správy. Na posledné štyri uvedené zraniteľnosti sú verejne dostupné exploity.

Zraniteľnosti CVE-2017-8731, CVE-2017-8734, CVE-2017-8750 a CVE-2017-11766 v prehliadači Edge spočívajú v chybnom prístupe ku objektom v pamäti. To môže útočník zneužiť na spôsobenie narušenia integrity pamäte, čím získa možnosť na diaľku vykonať škodlivý kód s právomocami práve prihláseného používateľa. Útočník potrebuje vytvoriť škodlivú webstránku, prípadne umiestniť škodlivý obsah na stránku so zdieľaným používateľským obsahom. Pre úspešné zneužitie útočník potrebuje používateľa nalákať na návštevu pripravenej stránky, napríklad prostredníctvom emailovej správy. Na prvé dve menované zraniteľnosti sú exploity verejne dostupné.

Ďalšie opravené kritické zraniteľnosti, CVE-2017-8741, CVE-2017-8748, CVE-2017-8649 a CVE-2017-8660, boli spôsobené chybami v JavaScript engine. Umožňujú útočníkovi spôsobením narušenia integrity pamäte vykonať na diaľku škodlivý kód s právomocami práve prihláseného používateľa. Pre úspešné zneužitie potrebuje útočník pripraviť škodlivú webovú stránku a nalákať používateľa na navštívenie danej stránky. Inými možnosťami je umiestnenie škodlivého obsahu na webovú stránku so zdieľaným používateľským obsahom, prípadne umiestnenie tohto obsahu do Microsoft Office dokumentu, otvorením ktorého rovnako dôjde ku zneužitiu zraniteľnosti.

Zraniteľnosti CVE-2017-8728 a CVE-2017-8737 vo Windows knižnici písiem, spočívajúcich v chybe pri narábaní s objektami v pamäti, čo môže útočník zneužiť na vykonanie škodlivého kódu s právomocami práve prihláseného používateľa. Útočník potrebuje vytvoriť škodlivý PDF súbor a umiestniť ho na webstránku, prípadne na stránku so zdieľaným používateľským obsahom. Pre úspešné zneužitie útočník potrebuje používateľa nalákať na návštevu pripravenej stránky. Inou možnosťou zneužitia zraniteľnosti je priame otvorenie škodlivého PDF súboru používateľom, čo je aj jediná možnosť na zariadeniach používajúcich iný internetový prehliadač ako Microsoft Edge.

Zraniteľnosti CVE-2017-8731 a CVE-2017-8751 v prehliadači Edge umožňujú útočníkovi zneužiť chybu v prístupe ku objektom v pamäti a tým spôsobiť narušenie integrity pamäte. To môže útočník zneužiť na vzdialené vykonanie škodlivého kódu s právomocami práve prihláseného používateľa. Pre úspešné zneužitie potrebuje útočník pripraviť škodlivú webovú stránku a nalákať používateľa na navštívenie danej stránky, napríklad pomocou emailu. Inou možnosťou je umiestnenie škodlivého obsahu na webovú stránku s používateľským obsahom.

Ďalšou opravenou kritickou zraniteľnosťou v prehliadači Edge je CVE-2017-8757, ktorá umožňuje útočníkovi spôsobením narušenia integrity pamäte vykonať na diaľku škodlivý kód s právomocami práve prihláseného používateľa. Pre úspešné zneužitie potrebuje útočník pripraviť škodlivú webovú stránku a nalákať používateľa na jej navštívenie. Inými možnosťami je umiestnenie škodlivého obsahu na webovú stránku so zdieľaným používateľským obsahom, prípadne umiestnenie tohto obsahu do Microsoft Office dokumentu, otvorením ktorého rovnako dôjde ku zneužitiu zraniteľnosti.

Zraniteľné systémy:

Microsoft Edge v systémoch Windows 10 verzií 1511, 1607 a 1730 v 32-bitových aj 64-bitových verziách
Microsoft Edge v systéme Windows Server 2016

Odporúčania:

Vzhľadom na vysoký počet verejne dostupných exploitov odporúčame čo najskôr aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov, a to 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-2017-11764
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8731
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8649
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8728
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8731
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8757

Mozilla Firefox

Spoločnosť Mozilla vydala v septembri opravy dvoch kritických zraniteľností v prehliadači Firefox.

Obe zraniteľnosti, CVE-2017-7811 a CVE-2017-7810, sa týkajú narušenia integrity pamäte a predpokladá sa, že to môže útočníkovi umožniť vykonanie škodlivého kódu. Pre zneužitie týchto zraniteľností je potrebné, aby užívateľ navštívil špeciálne pripravenú stránku.

Zraniteľné systémy:

Mozilla Firefox 55.03 a staršie
Mozilla Firefox ESR 52.3 a staršie

Odporúčania:

Odporúčame aktualizovať prehliadač Mozilla Firefox na verzie 56.0 a ESR 52.4. Prehliadač Firefox ponúka aktualizácie automaticky po ich zverejnení. Ak sa tak nestalo, aktualizáciu je možné spustiť manuálne otvorením Menu > Pomocník > O prehliadači Firefox. Kontrola aktualizácie sa spustí súčasne so zobrazením okna s informáciami o aktuálnej verzii.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/mfsa2017-21/
https://usn.ubuntu.com/usn/usn-3435-1/

Google Chrome

Spoločnosť Google v septembri vydala tri aktualizácie pre prehliadač Chrome. Detaily opráv v aktualizáciách sú uvedené iba pri prvej septembrovej aktualizácie (verzia 61.0.3163.79), ktorá obsahuje opravy šiestich dôležitých zraniteľností, a poslednej aktualizácii (verzia 61.0.3163.100), ktorá obsahuje opravu dvoch dôležitých zraniteľností a tretej zraniteľnosti, o ktorej nie sú zverejnené detaily.

Vo verzii 61.0.3163.79 boli opravené nasledujúce dôležité zraniteľnosti: CVE-2017-5111 – chyba v komponente PDFium umožňuje použitie už uvoľnenej pamäte; zraniteľnosti CVE-2017-5112 v komponente WebGL a CVE-2017-5113 v knižnici Skia môže útočník zneužiť na spôsobenie pretečenia zásobníka (heap); zraniteľnosť CVE-2017-5114 v komponente PDFium súvisí so správou pamäte (bližšie neurčené ako); zraniteľnosti CVE-2017-5115 a CVE-2017-5116 sú dôsledkom chyby vo V8 JavaScript engine umožňujúcej zámenou typov objektov.

Zraniteľnosti CVE-2017-5121 a CVE-2017-5122, opravené vo verzii 61.0.3163.100 a označené ako dôležité, sú spôsobené chybami vo V8 JavaScript engine a umožňujú útočníkovi prístup mimo pridelenú pamäť.

Zraniteľné systémy:
Google Chrome for Desktop 61.0.3163.91 a staršie (Windows, Mac a Linux)

Odporúčania:
Odporúčame overiť, či sa prehliadač Chrome automaticky aktualizoval na najnovšiu verziu 61.0.3163.100. Ak sa aktualizácia neudiala automaticky, odporúčame aplikovať aktualizáciu ručne cez menu otvorením okna s aktuálne nainštalovanou verziou, čo zároveň spustí aj kontrolu dostupnosti aktualizácie.

Zdroje:
https://chromereleases.googleblog.com/2017/10/stable-channel-updates-for-chrome-os.html
https://chromereleases.googleblog.com/2017/09/stable-channel-update-for-desktop_21.html
https://chromereleases.googleblog.com/2017/09/stable-channel-update-for-chrome-os.html
https://chromereleases.googleblog.com/2017/09/stable-channel-update-for-desktop.html

4. Adobe

Adobe Flash Player

Spoločnosť Adobe vydala v septembri opravy dvoch kritických zraniteľností v aplikáciách Adobe Flash Player.

Obe zraniteľnosti, CVE-2017-11281 a CVE-2017-11282, sa týkajú narušenia integrity pamäte. Po otvorení špeciálne pripraveného súboru môže útočník vykonať na používateľovom počítači škodlivý kód. K obom zraniteľnostiam existujú verejne dostupné exploity umožňujúce prístup mimo pridelenej pamäte.

Zraniteľné systémy:
Adobe Flash Player Desktop Runtime 26.0.0.151 a staršie (Windows, Macintosh a Linux)
Adobe Flash Player for Google Chrome 26.0.0.151 a staršie (Windows, Macintosh, Linux a Chrome OS)
Adobe Flash Player for Microsoft Edge and Internet Explorer 11 26.0.0.151 a staršie (Windows 10 a 8.1)

Odporúčania:
Vzhľadom na výskyt verejne dostupných exploitov odporúčame čo najskôr aktualizovať Adobe Flash Player na verziu 27.0.0.130. V závislosti od prehliadača a nastavení používateľa sa buď aktualizácia nainštaluje automaticky, zobrazením dialógového okna s upozornením, alebo je potrebné stiahnuť najnovšiu verziu zo stránok Adobe, viď posledný odkaz v sekcii zdroje.

Zdroje:
https://helpx.adobe.com/security/products/flash-player/apsb17-23.html
https://get.adobe.com/flashplayer/

5. Frameworky

Microsoft .NET

V rámci septembrového balíka aktualizácií vydala spoločnosť Microsoft opravu zero-day zraniteľnosti CVE-2017-8759 v .NET Framework, ktorá spočíva v chybe spracovania nedôveryhodného vstupu. Vzdialený útočník môže pomocou špeciálne pripravenej aplikácie, vyžívajúcej .NET Framework, prevziať plnú kontrolu nad zariadením. Pre úspešné zneužitie musí používateľ otvoriť pripravený škodlivý dokument, alebo škodlivú aplikáciu, pričom používateľské účty s menšími právomocami môžu byť zasiahnuté menej. Exploit na túto zraniteľnosť je verejne dostupný a bolo aj zaznamenané zneužívanie.

Zraniteľné systémy:
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 4.5.2
Microsoft .NET Framework 4.6
Microsoft .NET Framework 4.6.1
Microsoft .NET Framework 4.6.2
Microsoft .NET Framework 4.7

Odporúčania:
Vzhľadom na závažnosť uvedenej zraniteľnosti odporúčame čo najskôr aplikovať aktualizácie publikované prostredníctvom služby Windows Update.

Zdroje:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8759

Oracle Java SE

Spoločnosť Oracle v mesiaci september nevydala žiadne opravy zraniteľností. Najbližší balík opráv má byť vydaný 17. októbra 2017.

Zdroje:
http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html

6. Iné závažné zraniteľnosti

Kritická zraniteľnosť v Bluetooth

V septembri boli zverejnené informácie o kritickej zraniteľnosti, ktorá sa podľa odhadov týka až 5.3 miliardy zariadení využívajúcich protokol Bluetooth, ide najčastejšie o smartfóny, tlačiarne a smart televízie. Zraniteľnosť umožňuje útočníkovi vykonať útok typu man-in-the-middle a presmerovať všetku komunikáciu cez svoje zariadenie. Útočníkovi stačí nachádzať sa v dosahu Bluetooth signálu. Nie je potrebné predošlé spárovanie zariadení a zraniteľné zariadenie nemusí byť v móde "discoverable". Spoločnosť Microsoft už pre zariadenia využívajúce operačné systémy Windows vydala opravu (CVE-2017-8628). Ostatní výrobcovia vydávajú opravy svojich implementácií Bluetooth pod inými CVE označeniami. Napríklad v Linux kerneli je táto zraniteľnosť označená CVE-2017-1000251 a dôkaz existencie zraniteľnosti je verejne dostupný.

Zraniteľné systémy:
Foxit Reader 8.3.1 a staršie

Odporúčania:
Používateľom odporúčame preveriť svoje zariadenia a zistiť, či jeho výrobcovia, resp. dodávatelia operačného systému zverejnili opravy, a čo najskôr tieto opravy aplikovať.

Zdroje:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8628
https://threatpost.com/wireless-blueborne-attacks-target-billions-of-bluetooth-devices/127921/

Kritické zraniteľnosti v softvéri VMware

V mesiaci septembri vydala spoločnosť VMware opravu kritickej zraniteľnosti CVE-2017-4924, ktorá spočíva v zápise mimo pridelený rozsah pamäte na SVGA zariadení. Zneužitím tejto chyby môže hosťovský systém vykonať škodlivý kód na hostiteľskom systéme.

Zraniteľné systémy:

VMware ESXi 6.5
VMware Workstation 12.x
VMware Fusion 8.x

Odporúčania:

Odporúčame aplikovať aktualizácie: pre ESXi aktualizáciu ESXi650-201707101-SG, pre Workstation aktualizáciu na verziu 12.5.7, a pre Fusion odporúčame prechod na verziu 8.5.8.

Zdroje:

https://www.vmware.com/security/advisories/VMSA-2017-0015.html

Malvér zakompilovaný do softvéru CCleaner

V mesiaci septembri bola zverejnená informácia o prítomnosti malvéru v softvéri CCleaner, ktorý obsahoval funkcie na generovanie názvov domén, a tiež funkcionalitu na vzdialené ovládanie (C2 - Command and Control – charakteristické pre botnety) Útočníci napadli distribučné servery spoločnosti Avast a zneužili ich na distribúciu malvéru, pripojeného k inštalácii CCleaneru. Podľa odhadov bolo pred aplikovaním záplaty napadnutých až 2.3 milióna používateľských zariadení.

Zraniteľné systémy:

CCleaner 5.33

Odporúčania:

Odporúčame overiť nainštalovanú verziu CCleaner a bezodkladne aktualizovať na najnovšiu verziu 5.34. V prípade platených verzií sa záplata aplikuje automaticky, avšak v prípade verzií zadarmo je potrebné aktualizáciu vykonať manuálne.

Zdroje:

https://blog.avast.com/update-to-the-ccleaner-5.33.6162-security-incident