Mesačný prehľad kritických zraniteľností
Júl 2018

1. Operačné systémy Microsoft Windows

Tento mesiac spoločnosť Microsoft opravila zopár závažných zraniteľností.
Prvé štyri, ktoré spomenieme, sa týkajú zvýšenia práv. Zraniteľnosti CVE-2018-8282 a CVE-2018-8308 sú obidve spôsobené nesprávnym narábaním s objektmi v pamäti, na ktorých zneužitie musí byť útočník prihlásený v systéme a spustiť špeciálne upravenú aplikáciu. Ak sa mu toto podarí, získa možnosť vykonávať ďalší škodlivý kód a inštalovať programy, vidieť, meniť či mazať dáta, alebo vytvárať nové používateľské účty.
CVE-2018-8313 je ďalšou zraniteľnosťou zvýšenia práv a je spôsobená, keď Windows Kernel API vynucuje povolenia. Na zneužitie tejto zraniteľnosti je taktiež potrebné, aby lokálne autorizovaný útočník spustil špeciálne upravenú aplikáciu, čo mu potom dovolí zabraňovať komunikácii medzi procesmi, či prerušiť funkcionalitu systému. Poslednou z nich je CVE-2018-8314, ktorá umožňuje únik z testovacieho prostredia keď zlyhá kontrola. Túto zraniteľnosť je možné zneužiť spolu s inou zraniteľnosťou aby útočník získal možnosť vykonávať ľubovoľný kód.
Ďalej boli opravené tri zraniteľnosti narušenia dostupnosti systému CVE-2018-8309, CVE-2018-8304 a CVE-2018-8206. Prvá nastáva kvôli nesprávnemu narábaniu s objektmi v pamäti, pričom na jej zneužitie musí byť útočník prihlásený v systéme a spustiť špeciálne pripravenú aplikáciu. Druhá je spôsobená Windows Domain Name systémom keď DNSAPI.dl nesprávne spracuje DNS požiadavky. Na jej zneužitie je možné použiť škodlivý DNS server a poslať upravenú DNS požiadavku cieľu. Posledná sa týka nesprávneho narábania s FTP pripojeniami. Na zneužitie môže útočník poslať špeciálne pripravený paket počítaču s operačným systémom Windows, ktorý prijíma spojenia na TCP porte 21.
Zraniteľnosť CVE-2018-8222 umožňuje úspešnému útočníkovi vložiť škodlivý kód do procesu vykonávaného Windows PowerShellom. Na jej zneužitie musí útočník mať prístup k zariadeniu a vložiť škodlivý kód do skriptu, ktorý je overený politikou integrity kódu.
CVE-2018-8307 je spôsobená Microsoft WordPadom, ktorý nesprávne narába so vstavanými OLE objektmi. Jej zneužitie je možné pomocou špeciálne pripraveného dokumentu, pričom útočník musí presvedčiť používateľa, aby ho otvoril.

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 1703 for 32-bit Systems
Windows 10 Version 1703 for x64-based Systems
Windows 10 Version 1709 for 32-bit Systems
Windows 10 Version 1709 for x64-based Systems
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1803 for x64-based Systems
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 Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
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, version 1709 (Server Core installation)
Windows Server, version 1803 (Server Core installation)

Odporúčania:

Vzhľadom na množstvo kritických zraniteľností odporúčame bezodkladne 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-2018-8282
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8308
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8313
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8314
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8206
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8304
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8309
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8307
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8222

2. Kancelárske balíky Microsoft Office a Office Web Apps

V balíkoch Microsoft Office boli tento mesiac opravené štyri závažné zraniteľnosti.

CVE-2018-8312 a CVE-2018-8281 sú zraniteľnosti vzdialeného vykonávania kódu, obidve spôsobené nesprávnym narábaním s objektmi v pamäti. Na zneužitie môže útočník použiť špeciálne pripravený súbor. Potom musí ešte presvedčiť používateľa, aby ten súbor otvoril. To môže urobiť tak, že ho zašle pomocou e-mailu alebo rýchlej správy. Útočník môže taktiež

využiť špeciálne vytvorenú stránku, pričom odkaz na ňu pošle používateľovi, aby ho tak presvedčil nech ju navštívi. Po úspešnom zneužití jednej z týchto zraniteľností, môže útočník získať právo spúšťať škodlivý kód ako práve prihlásený používateľ. V prípade, že bol používateľ prihlásený ako administrátor získa útočník možnosť inštalovať programy, zobrazovať, meniť alebo mazať dáta, či vytvárať plnohodnotné účty.

Zraniteľnosti CVE-2018-8233 a CVE-2018-8299 sa týkajú zvýšenia práv, keď Microsoft SharePoint Server nesprávne spracuje špeciálne upravenú webovú požiadavku na SharePoint Server. Po úspešnom zneužití môže útočník vykonať cross-site scripting útoky na zraniteľných systémoch a spúšťať skripty ako práve prihlásený používateľ. To umožní útočníkovi čítať obsah, na ktorý nemá právo, vykonávať akcie v službe SharePoint ako daný používateľ (napríklad zmena alebo odstránenie obsahu, či vložiť škodlivý obsah do prehliadača používateľa).

Keď Skype for Business alebo Lync nesprávne rozdelia UNC cestu odkazu zdieľaného správou je možné zneužiť zraniteľnosť CVE-2018-8238. Zneužiť ju sa dá špeciálne pripraveným súborom, na ktorého odkaz musí používateľ kliknúť. Po jej zneužití získa útočník možnosť spúšťať príkazy ako práve prihlásený používateľ.

Zraniteľné systémy:

Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft Excel Viewer
Microsoft Office 2016 Click-to-Run (C2R) 32-bitová verzia
Microsoft Office 2016 Click-to-Run (C2R) 64-bitová verzia
Microsoft Office 2016 pre Mac
Microsoft Office Compatibility Pack Service Pack 3
Microsoft Office Word Viewer
Microsoft PowerPoint Viewer
Microsoft Access 2013 Service Pack 1 (32-bitová verzia)
Microsoft Access 2013 Service Pack 1 (64-bitová verzia)
Microsoft Access 2016 (32-bitová verzia)
Microsoft Access 2016 (64-bitová verzia)
Microsoft Office 2016 Click-to-Run (C2R) 32-bitová verzia
Microsoft Office 2016 Click-to-Run (C2R) 64-bitová verzia
Microsoft Lync 2013 Service Pack 1 (32-bitová verzia)
Microsoft Lync 2013 Service Pack (64-bitová verzia)
Skype for Business 2016 (32-bitová verzia)
Skype for Business (64-bitová verzia)

Odporúčania:

Vzhľadom množstvo závažných zraniteľností odporúčame bezodkladne 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-2018-8323
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8312
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8299
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8281
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8238

3. Internetové prehliadače

Microsoft Internet Explorer

Štyri kritické zraniteľnosti boli spoločnosťou Microsoft opravené v tohto-mesačnom balíku opráv. Zraniteľnosti sú spôsobené nesprávnym narábaním prehliadača Internet Explorer s objektmi v pamäti. Môžu spôsobiť také poškodenie pamäte, že útočník získa možnosť spúšťať kód ako práve prihlásený používateľ. Ak je teda práve prihláseným používateľom administrátor, získa útočník právo inštalovať programy, prezerať, mazať alebo meniť dáta, či vytvárať ďalšie plnohodnotné účty. Na ich zneužitie však útočník potrebuje interakciu používateľa, keďže ho musí presvedčiť aby navštívil špeciálne vytvorenú stránku, ktorej odkaz môže poslať napríklad pomocou emailu alebo rýchlej správy. Taktiež má možnosť vložiť do aplikácie alebo dokumentu Microsoft Office prvok ActiveX označený ako bezpečný na inicializáciu.

Zraniteľné systémy:
Microsoft Internet Explorer verzie 9, 10 a 11

Odporúčania:
Vzhľadom na závažnosť kritických zraniteľností odporúčame bezodkladne 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-2018-8296
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8291
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8288
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8242

Microsoft Edge

Dvanásť kritických zraniteľností bolo opravených tento mesiac v prehliadači Microsoft Edge, pričom všetky umožňujú vykonať škodlivý kód na diaľku.
Sú spôsobené tým, že skriptovací engine nesprávne narába s objektmi v pamäti. Zneužitie je možné len za pomoci používateľa, ktorého musí útočník presvedčiť k navštíveniu ním

špeciálne vytvorenej stránky. Úspešné zneužitie týchto zraniteľností umožňuje útočníkovi prebrať kontrolu nad systémom a vykonať ľubovoľný škodlivý kód s oprávneniami práve prihláseného používateľa. V prípade, že používateľ mal administrátorské práva útočník získa možnosť inštalovať programy, prezerať, meniť a mazať dáta, prípadne vytvárať plnohodnotné používateľské účty.

Zraniteľné systémy:

Microsoft Edge v systémoch Windows 10 verzií 1607, 1703, 1709 a 1803 a 32-bitových aj 64-bitových verziách
Microsoft Edge v systémoch Windows 10 32-bitových aj 64-bitových verziách
Microsoft Edge v systéme Windows Server 2016

Odporúčania:

Vzhľadom na množstvo kritických zraniteľností odporúčame bezodkladne 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-2018-8262
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8274
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8275
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8279
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8280
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8286
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8288
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8290
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8294
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8291
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8301
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8324

Mozilla Firefox

Spoločnosť Mozilla tento mesiac nevydala žiadne opravy zraniteľností v prehliadači Mozilla Firefox.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/

Google Chrome

Spoločnosť Google vydala aktualizácie prehliadača Chrome, ktoré obsahujú opravy 42 zraniteľností, z čoho 6 závažných.

Odporúčania:

Odporúčame overiť, či sa prehliadač Chrome automaticky aktualizoval na verziu 68.0.3440.75, prípadne novšiu. V prípade potreby odporúčame aplikovať aktualizáciu ručne cez menu otvorením okna s aktuálne nainštalovanou verziou, čo zároveň spustí aj kontrolu dostupnosti aktualizácie.

Zdroje:

https://chromereleases.googleblog.com/2018
https://chromereleases.googleblog.com/2018/07/stable-channel-update-for-desktop.html

4. Adobe Flash Player

Spoločnosť Adobe vydala tento mesiac aktualizácie pre Adobe Flash Player obsahujúce opravy kritickej zraniteľnosti CVE-2018-5007 umožňujúcej vzdialené vykonanie kódu a závažnej zraniteľnosti CVE-2018-5008 zverejňujúcej citlivé informácie. Vydala taktiež aktualizáciu pre Adobe Acrobat DC opravujúcu 52 kritických a 54 závažných zraniteľností týkajúcich sa vzdialeného vykonávania kódu, zvýšenia práv a zverejnenia citlivých informácií.

Zraniteľné systémy:

Adobe Flash Player Desktop Runtime 30.0.0.113 a staršie pre Windows, macOS aj Linux
Adobe Flash Player pre Google Chrome 30.0.0.113 a staršie
Adobe Flash Player pre Microsoft Edge a Internet Explorer 11 30.0.0.113 a staršie
Acrobat DC 2018.011.20040 a staršie
Acrobat Reader DC 2018.011.20040 a staršie
Acrobat 2017 2017.011.30080 a staršie
Acrobat Reader 2017 2017.011.30080 a staršie
Acrobat DC 2015.011.006.30418
Acrobat Reader DC 2015.011.006.30418

Odporúčania:

Používateľom odporúčame čo najskôr aktualizovať zraniteľné systémy nasledovne:

- Adobe Flash Player na verziu 30.0.0.134
- Acrobat DC 2018.011.20055
- Acrobat Reader DC 2018.011.20055
- Acrobat 2017 2017.011.30096
- Acrobat Reader 2017 2017.011.30096
- Acrobat DC 2015.011.006.30434
- Acrobat Reader DC 2015.011.006.30434

Aktualizácie sú dostupné prostredníctvom stránky Adobe Flash Player Download Center, prípadne prostredníctvom kontroly dostupných aktualizácii v produkte Adobe Flash Player.

Zdroje:

https://helpx.adobe.com/security/products/flash-player/apsb18-24.html
https://helpx.adobe.com/security/products/acrobat/apsb18-21.html

5. Frameworky

Microsoft .NET Framework

Pre Microsoft .NET Framework boli vydané aktualizácie, ktoré opravujú tri závažné zraniteľnosti.
Prvou je zraniteľnosť CVE-2018-8202 zvyšujúca práva, na ktorej zneužitie musí mať útočník prístup k zariadeniu a spustiť na ňom škodlivý program.
Zraniteľnosť CVE-2018-8356 nastáva keď komponenty .NET Frameworku nesprávne overia certifikáty.
Posledná opravená zraniteľnosť je CVE-2018-8284, ktorá tým, že nesprávne overí vstup umožní útočníkovi prevziať kontrolu nad systémom. Útočník potom môže inštalovať programy, prezerať, upravovať a mazať dáta, či vytvárať plnohodnotné účty.

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8202
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8356
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8284

Oracle Java

Veľká sada aktualizácii vydaná 17. júla 2018 spoločnosťou Oracle opravuje spolu osem zraniteľností pre Oracle Java SE z čoho jedna je kritická a tri sú označené ako závažné. Všetky opravené zraniteľnosti sa dajú zneužiť vzdialene bez overenia, čiže sa dajú využiť cez sieť bez vyžiadania užívateľského mena a hesla.

Zraniteľné systémy:

Java SE 10.0.1
Java SE 6u191, 7u181, 8u172
Java SE Embedded 8u171
JRockit R28.3.18

Odporúčania:

Vzhľadom na závažnosť uvedených zraniteľností odporúčame čo najskôr aktualizovať zraniteľné verzie Java SE a Java SE Embedded na aktuálne verzie, t.j. Java SE 8u181, Java 10.0.2 a Java SE Embedded 8u181, prostredníctvom Java Auto Update, alebo na stránke spoločnosti Oracle, viď prvý odkaz v zdrojoch.

Zdroje:

https://www.oracle.com/downloads/index.html#java
http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html

6. Iné závažné zraniteľnosti

NetSpectre

Bol objavený útok založený na zraniteľnosti Spectre 1, pričom momentálne je možné bez vzdialeného vykonávania kódu alebo využitia cache pamäte získať 60 bitov údajov z pamäte za hodinu. Pre bližšie informácie si pozrite naše varovanie.

Zraniteľné systémy:
Zariadenia využívajúce Intel, AMD a ARM procesory a zároveň LAN siete, Virtuálne systémy Google Cloud

Odporúčania:
Odporúčame aktualizovať prehliadače na najnovšiu verziu

Cisco

V Cisco IP telefónoch, Cisco FireSIGHT System softvéri a Cisco StarOS boli odhalené zraniteľnosti spôsobujúce vzdialené vykonávanie kódu a injekciu príkazov. Viac informácií môžete získať v našom varovaní.

Zraniteľné systémy:
IP Phone 6800 Series with Multiplatform Firmware
IP Phone 7800 Series with Multiplatform Firmware
IP Phone 8800 Series with Multiplatform Firmware
Cisco FireSIGHT System Software
Cisco Web Security Appliance
Cisco Virtualized Packet Core-Single Instance (VPC-SI)
Cisco Virtualized Packet Core-Distributed Instance (VPC-DI)
Cisco Ultra Packet Core (UPC)

Odporúčania:
- **CVE-2018-0341**
  Táto zraniteľnosť bude opravená v auguste 2018 vo verzii 11.2(1). Aktualizácie budú dostupné na Cisco Software Center na Cisco.com, kde to budete môcť nájsť pod ***Products > Collaboration Endpoints > IP Phones > IP Phones with Multiplatform Firmware.***
- **CVE-2018-0369**
  Na zistenie či je na zariadení zraniteľná verzia Cisco StarOS môžu administrátori použiť príkaz ***show version***.
  Odporúčame mať aktualizované všetky zraniteľné systémy na najnovšie verzie, ktoré môžete sledovať tu.

Zraniteľnosti procesorov Spectre 1.1 a 1.2

Nové objavené zraniteľnosti procesorov Intel, ARM a AMD umožňujú získať citlivé údaje z operačnej pamäte procesora. Pre bližšie informácie si pozrite naše varovanie.

Zraniteľné systémy:
Procesory Intel (overené)
ARM (overené niektoré)
AMD

Odporúčania:
Aplikovať aktualizácie operačných systémov
Aplikovať Microcode / BIOS aktualizácie