Mesačný prehľad kritických zraniteľností
Jún 2018

1. Operačné systémy Microsoft Windows

V júnovej sade aktualizácií od spoločnosti Microsoft boli opravené štyri kritické zraniteľnosti. Tri z toho umožňujú vzdialené vykonávanie kódu. Konkrétne CVE-2018-8213 je spôsobená nesprávnym narábaním Windowsu s objektmi v pamäti pričom útočník sa na jej zneužitie musí najprv prihlásiť do systému a tak spustiť špeciálne pripravenú aplikáciu.
V prípade zraniteľnosti CVE-2018-8231 sa jedná o to, že http Protocol Stack (http.sys) nesprávne narába s objektmi v pamäti. Na zneužitie stačí, ak neautentifikovaný útočník pošle špeciálne upravený paket zraniteľnému Http.sys serveru.
Poslednou zraniteľnosťou vzdialeného vykonávania ľubovoľného kódu je zraniteľnosť CVE-2018-8225, ktorá je spôsobená nesprávnym spracovaním DNS odpovedí DNSAPI.dll. Na jej zneužitie môže útočník využiť škodlivý DNS server, ktorý bude posielať škodlivé DNS odpovede systému.
Poslednou kritickou zraniteľnosťou opravenou tento mesiac je zraniteľnosť poškodenia pamäte CVE-2018-8251, ktorá nastáva pri nesprávnom narábaní Windows Media Foundation s objektmi v pamäti. Na jej zneužitie musí útočník presvedčiť používateľa, aby otvoril špeciálne pripravený súbor alebo navštívil útočníkom upravenú stránku. Po úspešnom zneužití má útočník možnosť inštalovať programy, pozerať meniť či mazať dáta alebo aj vytvárať nové používateľské kontá.

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-2018-8213
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8231
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8225
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8251

2. Kancelárske balíky Microsoft Office a Office Web Apps

V balíkoch Microsoft Office sa tento mesiac opravilo sedem závažných zraniteľností z čoho štyri sa týkajú zvýšenia práv. Medzi nimi je zraniteľnosť CVE-2018-8244, ktorá je spôsobená nedostatočným overovaním hlavičiek príloh Microsoft Outlooku a po zneužití umožní útočníkovi posielať e-maily so skrytými prílohami, ktoré sa potom otvoria či spustia.
Ďalšou z týchto závažných zraniteľností je CVE-2018-8247, ktorá existuje preto, že Office Web Apps Server 2013 a Office Online Server nesprávne spracúvajú webové požiadavky. Posledné dve z nich, CVE-2018-8252 a CVE-2018-8254, sa týkajú Microsoft SharePoint Servera, ktorý nesprávne spracúva špeciálne vytvorené webové požiadavky naň. Útočník túto zraniteľnosť môže zneužiť poslaním špeciálne upravenej URL adresy používateľovi zasiahnutého SharePoint servera. Po úspešnom zneužití niektorej z týchto zraniteľností 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).
CVE-2018-8146 je ďalšou opravenou závažnou zraniteľnosťou, táto sa však týka úniku citlivých informácií. Konkrétne ide o produkt Microsoft Excel, ktorý nesprávne zverejňuje obsah svojej pamäte. Útočník na zneužitie potrebuje presvedčiť používateľa aby otvoril

špeciálne vytvorený dokument, ktorý mu môže poslať napríklad e-mailom. Útočník v tomto prípade potrebuje poznať miesto, kde bol objekt vytvorený v pamäti.

Spomenieme ešte tri zraniteľnosti týkajúce sa vzdialeného vykonávania kódu. Prvou je zraniteľnosť s označením CVE-2018-8245, ktorá vzniká keď Microsoft Publisher neuzamkne zónu lokálneho počítača pri inštancovaní OLE objektov. Na jej zneužitie musí používateľ otvoriť dokument, ktorý dostal napríklad e-mailom od útočníka v aplikácii Publisher.

CVE-2018-8248 sa týka Microsoft Excelu, ktorý nesprávne narába s objektmi v pamäti a CVE-2018-8176, ktorá nastáva keď Microsoft PowerPoint nezvládne správne overiť XML obsah. Útočník na ich zneužitie môže použiť špeciálne vytvorenú stránku, no musí presvedčiť používateľa, aby ju navštívil. To môže urobiť zaslaním mailu alebo okamžitej správy s odkazom, na ktorý má používateľ kliknúť. Prípadne by mohol útočník využiť aj špeciálne vytvorený súbor navrhnutý na zneužitie zraniteľnosti. Aj v tomto prípade však musí útočník presvedčiť používateľa aby otvoril súbor. Pri úspešnom zneužití niektorej 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.

Zraniteľné systémy:

Microsoft Sharepoint enerprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft Office Compatibility Pack Service Pack 3
Microsoft Office Web Apps 2013 Service Pack 1
Microsoft Office 2016 for Mac
Microsoft Office Online Server 2016
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 Click-to-run (C2R) for 32-bit editions
Microsoft Office 2016 Click-to-run (C2R) for 64-bit editions
Microsoft Outlook 2013 RT Service Pack 1 (32-bit edition)
Microsoft Outlook 2013 RT Service Pack 1 (64-bit edition)
Microsoft Outlook 2016 (32-bit edition)
Microsoft Outlook 2016 (64-bit edition)
Microsoft Excel 2010 Service Pack 2 (32-bit editions)
Microsoft Excel 2010 Service Pack 2 (64-bit editions)
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)

Microsoft Excel Viewer

Odporúčania:

Vzhľadom na 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-2018-8244
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8247
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8252
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8254
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8246
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8245
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8176
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8248

3. Internetové prehliadače

Microsoft Internet Explorer

Iba dve kritické zraniteľnosti boli spoločnosťou Microsoft opravené v tohto-mesačnom balíku opráv. Obe 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 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-2018-8267
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8249

Microsoft Edge

Štyri kritické zraniteľnosti boli opravené 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-2018-8110
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8111
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8229
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8236

Mozilla Firefox

Spoločnosť Mozilla v júni vydala aktualizácie opravujúce len jednu závažnú zraniteľnosť s označením CVE-2018-6126. Nastáva keď knižnica Skia rasterizuje cesty za použitia poškodeného SVG súboru s vypnutou funkciou anti-aliasing.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-14/

Google Chrome

Spoločnosť Google vydala aktualizácie prehliadača Chrome, ktoré obsahujú opravy dvoch závažných bezpečnostných zraniteľností.

Odporúčania:

Odporúčame overiť, či sa prehliadač Chrome automaticky aktualizoval na verziu 66.0.3359.170, 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/2018/06/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2018/06/stable-channel-update-for-desktop_12.html

4. Adobe Flash Player

Tento mesiac boli vydané aktualizácie na dve kritické zraniteľnosti CVE-2018-4945 a CVE-2018-5002 v Adobe Flash Playeri verzie 29.0.0.171 a starších. Tieto zraniteľnosti môžu spôsobiť spustenie kódu ako práve prihlásený používateľ pričom Adobe dostalo správu že zraniteľnosť označená ako CVE-2018-5002 bola využitá voči užívateľom Windowsu zasielaním dokumentov so škodlivým obsahom e-mailom. Okrem toho boli tento mesiac vydané záplaty na ešte dve kritické zraniteľnosti o ktorých sa môžete dočítať viac v našom varovaní.

Zraniteľné systémy:
Adobe Flash Player Desktop Runtime 29.0.0.171 a staršie pre Windows, macOS aj Linux
Adobe Flash Player pre Google Chrome 29.0.0.171 a staršie
Adobe Flash Player pre Microsoft Edge a Internet Explorer 29.0.0.171 a staršie

Odporúčania:
Používateľom odporúčame čo najskôr aktualizovať zraniteľné systémy. Jedná sa najmä. o Adobe Flash Player, ktorý treba aktualizovať na verziu 30.0.0.113. 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/apsb18-19.html

5. Frameworky

Microsoft .NET Framework

Pre Microsoft .NET Framework neboli v mesiaci jún vydané žiadne aktualizácie opravujúce zraniteľnosti.

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

Oracle Java

Spoločnosť Oracle nevydala v mesiaci jún žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 17. júl 2018.

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

6. Iné závažné zraniteľnosti

Wavetrough

Zraniteľnosť týkajúca sa prehliadača Microsoft Edge a vývojovej verzie Mozilla Firefox umožňuje čítať obsah stránok, kde je používateľ prihlásený. Pre bližšie informácie si pozrite naše varovanie.

Zraniteľné systémy:

Microsoft Edge
Mozilla Firefox – vývojová verzia Nightly 59.0b9

Odporúčania:

Odporúčame aktualizovať prehliadače na najnovšiu verziu

Zraniteľnosť Cortany vo Windows 10

V systémoch používajúcich Windows 10 bola objavená zraniteľnosť, ktorú spôsobuje služba Cortana a umožňuje zvýšenie práv a vykonávanie škodlivého kódu. Viac informácií môžete získať v našom varovaní.

Zraniteľné systémy:

Microsoft Windows 10 Version 1803 for x64-based Systems
Microsoft Windows 10 Version 1803 for 32-bit Systems
Microsoft Windows 10 version 1709 for x64-based Systems
Microsoft Windows 10 version 1709 for 32-bit Systems

Odporúčania:

Odporúčame vypnúť službu Cortana, čo zabráni zneužitiu tejto zraniteľnosti a taktiež aplikovať aktualizácie vydané spoločnosťou Windows. Číslo aktualizácie pre konkrétny systém možno vyhľadať tu vložením identifikátora zraniteľnosti (CVE-2018-8140) do príslušného poľa vyhľadávania.

SigSpoof

Táto zraniteľnosť sa týka elektronického podpisovania e-mailov a môže viesť k dezinformácii používateľa a zvýšenej účinnosti phishingu. Pre bližšie informácie si pozrite naše varovanie.

Zraniteľné systémy:

GnuPG s verziou nižšou ako 2.2.8
GnuPG s verziou nižšou ako 1.4.23
Enigmail s verziou nižšou ako 2.0.7
GPGTools s verziou nižšou ako 2018.3
python-gnupg s verziou nižšou ako 0.4.3
pass s verziou nižšou ako 1.7.2

Odporúčania:

Odporúčame aktualizovať softvér nasledovne:

- GnuPG aspoň na verziu 2.2.8 alebo 1.4.23

- Enigmail aspoň na verziu 2.0.7
- GPGTools aspoň na verziu 2018.3
- python-gnupg aspoň na verziu 0.4.3
- pass aspoň na verziu 1.7.2