Mesačný prehľad kritických zraniteľností
August 2018

1. Operačné systémy Microsoft Windows

Štyri kritické zraniteľnosti týkajúce sa operačného systému Windows boli tento mesiac opravené spoločnosťou Microsoft. Každá z týchto zraniteľností umožňuje útočníkovi vzdialene vykonávať kód.
Prvou je zraniteľnosť CVE-2018-8345, ktorej zneužitie nastáva, keď je spustený súbor .LNK. Na to, aby útočník dostal .LNK súbor do cieľového systému môže poskytnúť používateľovi vymeniteľný disk alebo zdieľanú zložku so škodlivým súborom.
Kritická zraniteľnosť CVE-2018-8350 nastáva, keď Microsoft Windows PDF Library nesprávne narába s objektmi v pamäti. Pri nastavení hlavného prehliadača Microsoft Edge na systémoch Windows 10 je možné zneužiť túto zraniteľnosť iba prezretím stránky, ktorá je špeciálne upravená a obsahuje škodlivý PDF obsah. Ostatné prehliadače neposkytujú automaticky PDF obsah, takže útočník nemá možnosť ako donútiť používateľa aby otvoril súbor. Namiesto toho, však môže súbor poslať ako prílohu v e-maile alebo rýchlej správe.
Dve zraniteľnosti CVE-2018-8344 a CVE-2018-8397 taktiež umožňujú vzdialené vykonávanie kódu. Prvá zo spomenutých nastáva nesprávnym spracovaním špeciálne vytvorených písem knižnicou písiem systému Windows. Druhá z nich je spôsobená nesprávnym spracúvaním objektov v pamäti grafickým rozhraním systému Windows (GDI). Útočník, ktorý úspešne zneužije niektorú z týchto zraniteľností, by mohol prevziať kontrolu nad postihnutým systémom. Útočník potom môže nainštalovať programy; zobraziť, zmeniť alebo vymazať údaje; alebo vytvoriť nové účty s plnými používateľskými právami. Používatelia, ktorých účty sú nakonfigurované tak, aby mali menej používateľských práv v systéme, by mohli byť menej ovplyvnené ako používatelia, ktorí pracujú s administrátorskými používateľskými právami. Na ich zneužitie musí útočník presvedčiť používateľa, aby navštívil špeciálne pripravenú stránku, alebo otvoril špeciálne upravený dokument. To môže urobiť tým, že zašle odkaz na stránku alebo súbor používateľovi pomocou e-mailu alebo rýchlej správy.
Okrem týchto kritických zraniteľností opravila spoločnosť Microsoft aj jednu závažnú zraniteľnosť, ktorá je aktívne zneužívaná. Viac sa o nej môžete dočítať v našom varovaní.
Koncom mesiaca bola objavená aj zero-day zraniteľnosť, ktorá funguje aj na najaktuálnejšom operačnom systéme Windows 10 v 64-bitovej verzii. Zraniteľnosť spočívajúca v Windows plánovači úloh pri chybách v narábaní s Advanced Local Procedure Call (ALPC) umožňuje zvýšenie práv.

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 a aktívne zneužívanú zraniteľnosť 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-2018-8344
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8345
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8350
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8397
https://thehackernews.com/2018/08/windows-zero-day-exploit.html

2. Kancelárske balíky Microsoft Office a Office Web Apps

V balíkoch Microsoft Office bolo tento mesiac opravených šesť závažných zraniteľností. Zraniteľnosti označené ako CVE-2018-8375, CVE2018-8376 a CVE-2018-8379 sú všetko zraniteľnosti vzdialeného vykonávania kódu spôsobené tým, že Microsoft Excel alebo Microsoft PowerPoint nesprávne narába s objektmi v pamäti. Na zneužitie môže útočník použiť špeciálne pripravený súbor. Potom musí ešte presvedčiť používateľa, aby tento 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 s cieľom presvedčiť ho, aby ju navštívil. 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.

Zraniteľnosť CVE-2018-8412 sa týka zvýšenia práv, keď Microsoft AutoUpdate (MAU) pre Mac nesprávne overí aktualizácie pred ich spustením. Po zneužití môže útočník vykonať kód v systéme a získať zvýšené práva.
Posledné dve opravené zraniteľnosti CVE-2018-8378 a CVE-2018-8382 umožňujú únik informácií. Prvá zraniteľnosť nastáva, keď Microsoft Office načíta pamäť mimo rozsahu kvôli neinicializovanej premennej a umožní tak útočníkovi vidieť obsah mimo rozsahu. Druhá nastáva, keď Microsoft Excel nesprávne zverejní obsah pamäte, ktorý útočník môže zneužiť.

Zraniteľné systémy:

Microsoft Excel 2016 Click-to-run 32-bitová verzia
Microsoft Excel 2016 Click-to-run 64-bitová verzia
Microsoft Excel 2010 Service Pack 2 (32-bitová verzia)
Microsoft Excel 2010 Service Pack 2 (64-bitová verzia)
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bitová verzia)
Microsoft Excel 2013 Service Pack 1 (64-bitová verzia)
Microsoft Excel 2016 (32-bitová verzia)
Microsoft Excel 2016 (64-bitová verzia)
Microsoft Excel Viewer 2007 Service Pack 3
Microsoft Office 2016 pre Mac
Microsoft Office Compatibility Pack Service Pack 3
Microsoft PowerPoint 2010 Service Pack 2 (32-bitová verzia)
Microsoft PowerPoint 2010 Service Pack 2 (64-bitová verzia)
Microsoft Office 2016 Click-to-Run (C2R) 32-bitová verzia
Microsoft Office 2016 Click-to-Run (C2R) 64-bitová verzia
Microsoft Office 2010 Service Pack 2 (32-bitová verzia)
Microsoft Office 2010 Service Pack 2 (64-bitová verzia)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bitová verzia)
Microsoft Office 2013 Service Pack 1 (64-bitová verzia)
Microsoft Office 2016 (32-bitová verzia)
Microsoft Office 2016 (64-bitová verzia)
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2013 Service Pack 1
Microsoft Office Web Apps 2010 Service Pack 2
Microsoft Office Web Apps 2013 Service Pack 1
Microsoft Office Word 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-2018-8375
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8376
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8379
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8378
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8382
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8412

3. Internetové prehliadače

Microsoft Internet Explorer

Šesť kritických zraniteľností týkajúcich sa prehliadača Internet Explorer bolo v tomto mesiaci opravených spoločnosťou Microsoft. Opravené boli zraniteľnosti s označením: CVE-2018-8373, CVE-2018-8385, CVE-2018-8403, CVE-2018-8355, CVE-2018-8371 a CVE-2018-8372.
O zraniteľnosti s označením CVE-2018-8373 sa môžete dozvedieť bližšie informácie aj v našom varovaní.
Zraniteľnosti sú spôsobené nesprávnym narábaním prehliadača Internet Explorer s objektmi v pamäti. Môžu spôsobiť také poškodenie pamäte, vďaka ktorému 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 a 11

Odporúčania:

Vzhľadom na množstvo a 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-2018-8355
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8371
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8372
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8373
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8385
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8403

Microsoft Edge

Desať kritických zraniteľností bolo opravených tento mesiac v prehliadači Microsoft Edge, pričom všetky umožňujú vykonať škodlivý kód na diaľku.
Všetky zraniteľnosti sú spôsobené tým, že skriptovací nástroj 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-2018-8372
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8266
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8355
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8377
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8387
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8390
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8403
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8381
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8385
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8380

Mozilla Firefox

Spoločnosť Mozilla tento mesiac opravila päť kritických a štyri závažné zraniteľnosti. Zraniteľnosti označené ako kritické môžete nájsť pod označeniami CVE-2018-12359, CVE-2018-12360, CVE-2018-12361, CVE-2018-5189 a CVE-2018-5188. Môžu spôsobiť vzdialené vykonávanie kódu, či spadnutie systému, ktoré je možné ďalej zneužiť.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-19/

Google Chrome

Spoločnosť Google nevydala tento mesiac žiadne aktualizácie opravujúce kritické alebo závažné zraniteľnosti.

Zdroje:

https://chromereleases.googleblog.com/2018

4. Adobe Flash Player

Spoločnosť Adobe vydala tento mesiac aktualizácie pre Adobe Flash Player obsahujúce opravy piatich závažných zraniteľností. Opravené zraniteľnosti sú označené ako CVE-2018-12824, CVE-2018-12825, CVE-2018-12826, CVE-2018-12827 a CVE-2018-12828 a môžu spôsobiť únik informácií či zvýšenie práv.
Spoločnosť vydala taktiež aktualizáciu pre Adobe Acrobat DC, ktorá opravuje dve kritické zraniteľnosti. Obe zraniteľnosti umožňujú vzdialené vykonávanie kódu a nájsť ich môžete pod označeniami CVE-2018-12808 a CVE-2018-12799.

Zraniteľné systémy:

Adobe Flash Player Desktop Runtime 30.0.0.134 a staršie pre Windows, macOS aj Linux
Adobe Flash Player pre Google Chrome 30.0.0.134 a staršie
Adobe Flash Player pre Microsoft Edge a Internet Explorer 11 30.0.0.134 a staršie
Acrobat DC 2018.011.20055 a staršie
Acrobat Reader DC 2018.011.20055 a staršie
Acrobat 2017 2017.011.30096 a staršie
Acrobat Reader 2017 2017.011.30096 a staršie
Acrobat DC 2015 2015.006.30434
Acrobat Reader DC 2015 2015 2015.006.30434

Odporúčania:

Používateľom odporúčame čo najskôr aktualizovať zraniteľné systémy nasledovne:

- Adobe Flash Player na verziu 30.0.0.154
- Acrobat DC 2018.011.20058
- Acrobat Reader DC 2018.011.20058
- Acrobat 2017 2017.011.30099
- Acrobat Reader 2017 2017.011.30099

- Acrobat DC 2015 2015.006.30448
- Acrobat Reader DC 2015 2015.006.30448

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

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/acrobat/apsb18-29.html
https://helpx.adobe.com/security/products/flash-player/apsb18-25.html

5. Frameworky

Microsoft .NET Framework

Jedna závažná zraniteľnosť bola opravená v aktualizácii vydanej pre Microsoft .NET Framework. CVE-2018-8360 je zraniteľnosť umožňujúca únik informácií, ktorá môže nastať pri používaní .NET Frameworku v sieťových pripojeniach s vysokou záťažou či vysokou hustotou. Zneužitie tejto zraniteľnosti môže spôsobiť zobrazenie údajov medzi zákazníkmi. Keď teda útočník má prístup k zákazníkovi v takej sieti, mohol by vidieť údaje iných zákazníkov.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8360

Oracle Java

Spoločnosť Oracle nevydala v mesiaci jún žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 16. október 2018.

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

6. Iné závažné zraniteľnosti

ForeShadow

Boli odhalené nové zraniteľnosti procesorov Intel, ktoré umožňujú útočníkovi získať dáta z pamäte. Viac informácií môžete nájsť v našom varovaní.

Zraniteľné systémy:
Procesory z radu Intel Core a Xeon

Odporúčania:
Inštalácia záplat na firmware a operačný systém.

Zraniteľnosť v PHP

Redakčné systémy využívajúce PHP postihla zraniteľnosť objavená v jazyku PHP. Využitie zraniteľnosti umožňuje vykonávať ľubovoľný kód na cieľovom serveri. Pre viac informácií si prečítajte naše varovanie.

Zraniteľné systémy:

Wordpress

Typo3

Knižnica TCPDF

Iné nešpecifikované CMS využívajúce jazyk PHP

Odporúčania:

- **Wordpress**
  Aktualizácia neodstraňuje problém úplne.
- **Typo3**
  Aktualizácia aspoň na verziu 7.6.30, 8.7.17 a 9.3
- **TCPDF**
  Zatiaľ neopravené

Zraniteľnosť frameworku Apache Struts 2

Pri pomerne bežnej konfigurácii umožňuje zraniteľnosť frameworku Apache Struts vzdialené vykonávanie kódu. Pre viac informácií si prečítajte naše varovanie.

Zraniteľné systémy:

Apache Struts 2 verzie 2.3 – 2.3.34 a 2.5 – 2.5.16

Odporúčania:

Aktualizácia na verziu 2.3.35, alebo 2.5.17