Mesačný prehľad kritických zraniteľností

Október 2017

1. Operačné systémy Microsoft Windows

V mesiaci október vydala spoločnosť Microsoft opravy 7 kritických zraniteľností v operačných systémoch Windows.

Kritické zraniteľnosti CVE-2017-11762 a CVE-2017-11763 umožňujú útočníkovi na diaľku vykonať škodlivý kód. K chybe môže dôjsť keď knižnica písem systému Windows nesprávne spracuje špeciálne vytvorené vstavané písma. Úspešným zneužitím môže útočník prevziať kontrolu nad napadnutým systémom, inštalovať programy, prehliadať, meniť a zmazať dáta, a vytvárať nové užívateľské kontá s právomocami práve prihláseného používateľa. Pre zneužitie zraniteľností je potrebné, aby bol používateľ nalákaný otvoriť špeciálne pripravenú webovú stránku, kliknúť na odkaz na túto stránku umiestnený napríklad v emaili alebo otvoriť špeciálne pripravený škodlivý súbor, zaslaný napríklad emailom.

Kritická zraniteľnosť CVE-2017-8727 umožňuje útočníkovi na diaľku vykonať škodlivý kód. K chybe môže dôjsť keď Internet Explorer nesprávne pristúpi k objektom v pamäti cez Microsoft Windows Text Services Framework. Zraniteľnosť môže zapríčiniť narušenie integrity pamäte tak, že to môže viesť k vykonaniu škodlivého kódu s právomocami práve prihláseného používateľa. Ak je užívateľ prihlásený ako správca, môže útočník prevziať kontrolu nad napadnutým systémom. Pre úspešné zneužitie zraniteľnosti musí byt používateľ nalákaný na webovú stránku so špeciálne pripraveným škodlivým obsahom.

Kritická zraniteľnosť CVE-2017-11771 umožňuje útočníkovi na diaľku vykonať škodlivý kód. K chybe môže dôjsť pri správe objektov v pamäti servisom Windows Search. Úspešné zneužitie tejto zraniteľnosti môže viesť k prevzatiu kontroly útočníkom nad napadnutým systémom. Pre úspešné zneužitie zraniteľnosti musí útočník poslať špeciálne pripravenú správu servisu Windows Search. Útočník s prístupom k cieľovému počítaču môže využiť túto zraniteľnosť na povýšenie právomocí a prebratie kontroly nad systémom. Navyše je aj možnosť vzdialeného útoku, keď neautorizovaný útočník vzdialene zneužije zraniteľnosť cez SMB pripojenie a preberie kontrolu nad systémom.

Kritická zraniteľnosť CVE-2017-11779 je v komponente Windows DNS (DNSAPI.dll) a umožňuje útočníkovi na diaľku vykonať škodlivý kód, ak Windows DNS zlyhá v správe DNS odozvy. Útočník úspešným zneužitím zraniteľnosti získa práva účtu Local System. Pre úspešné zneužitie zraniteľnosti musí útočník použiť škodlivý DNS server na zaslanie DNS odozvy cieľovému systému.

Kritická zraniteľnosť CVE-2017-11819 umožňuje útočníkovi na diaľku vykonať škodlivý kód. Chyba spočíva v spôsobe prístupu k objektom v pamäti prehliadačmi od spoločnosti Microsoft. Zraniteľnosť môže zapríčiniť narušenie integrity pamäte tak, že to môže viesť k vykonaniu škodlivého kódu s právomocami práve prihláseného používateľa. Ak je užívateľ prihlásený ako správca, môže to znamenať prevzatie kontroly nad napadnutým systémom. Pre úspešné zneužitie zraniteľnosti musí útočník vytvoriť špeciálnu webovú stránku a nalákať používateľa na stránku so týmto škodlivým obsahom.

Pre zraniteľnosť CVE-2017-11785, ktorá je označená ako dôležitá, už existuje verejne dostupný exploit. Zraniteľnosť je spôsobená chybou vo Windows kerneli a môže spôsobiť únik informácií, s ktorými útočník môže obísť randomizáciu kernelového adresového priestoru. Týmto získa informácie, ktoré môže ďalej zneužiť pri pokračovaní útoku. Pre úspešné zneužitie tejto zraniteľnosti sa útočník musí lokálne prihlásiť do systému a spustiť špeciálne pripravenú aplikáciu.

Ďalšou zraniteľnosťou, ktorá bola označená ako dôležitá a je pre ňu verejne dostupný exploit, je CVE-2017-11823. Týka sa všetkých verzií systémov Windows 10 a oboch verzií systémov Windows Server 2016. Táto zraniteľnosť umožňuje obídenie bezpečnostných prvkov chybou vo Windows PowerShell. Úspešné zneužitie tejto zraniteľnosti umožní útočníkovi vložiť škodlivý kód do dôveryhodného procesu v PowerShell a obísť tak politiku ochrany integrity kódu zariadenia na lokálnom systéme. Pre úspešné zneužitie tejto zraniteľnosti musí mať útočník prístup k lokálnemu systému a vložiť škodlivý kód do skriptu, ktorý je dôveryhodný pre politiku integrity kódu.

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 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)

Odporúčania:

Vzhľadom na závažnosť niektorých uvedených 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-2017-8727
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11762
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11763
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11771
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11779
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11819
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11785
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11823

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft v rámci októbrového balíka aktualizácií nevydala vydala opravu žiadnej kritickej zraniteľnosti, avšak sú správy o aktívnom zneužívaní zraniteľnosti CVE-2017-11826 (viď posledný odkaz v sekcii zdroje), ktorá je označená len ako dôležitá.

Táto zraniteľnosť spočíva v narušení integrity pamäte, keď v softvéri zlyhá správa objektov v pamäti. Úspešné zneužitie umožní útočníkovi na diaľku vykonať škodlivý kód s právomocami práve prihláseného používateľa. Útočník môže tiež inštalovať programy, prehliadať, meniť a zmazať dáta, a vytvárať nové užívateľské kontá s právomocami práve prihláseného používateľa. Pre zneužitie zraniteľnosti je potrebné, aby používateľ otvoril špeciálne pripravený súbor so zraniteľnou verziou Microsoft Office-u. Takýto škodlivý súbor môže byť zaslaný v prílohe emailu, umiestnený na webovej stránke, avšak v oboch prípadoch je pre úspešne zneužitie tejto zraniteľnosti nutné nalákať používateľa na otvorenie tohto súboru.

Zraniteľné systémy:
Microsoft Office Compatibility Pack Service Pack 3
Microsoft Office Online Server 2016
Microsoft Office Web Apps Server 2010 Service Pack 2
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft Office Word Viewer
Microsoft SharePoint Enterprise Server 2016
Microsoft Word 2007 Service Pack 3
Microsoft Word 2010 Service Pack 2 (32-bit and 64-bit editions)
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bit and 64-bit editions)
Microsoft Word 2016 (32-bit edition)
Word Automation Services (platform Microsoft SharePoint Server 2010 Service Pack 2)
Word Automation Services (platform Microsoft SharePoint Server 2013 Service Pack 1)

Odporúčania:
Vzhľadom na aktívne zneužívanie uvedenej zraniteľnosti 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-2017-11826
https://threatpost.com/microsoft-patches-office-bug-actively-being-exploited/128367/

3. Internetové prehliadače

Microsoft Internet Explorer

V rámci októbrového balíka opráv boli spoločnosťou Microsoft vydané opravy 4 kritických zraniteľností v internetových prehliadačoch Internet Explorer. Všetky z týchto zraniteľností umožňujú útočníkovi na diaľku vykonať škodlivý kód.

Kritické zraniteľnosti CVE-2017-11793 a CVE-2017-11810 sú dôsledkom spôsobu, akým skriptovací engine spravuje objekty v pamäti. Pre úspešné zneužitie zraniteľností musí byť užívateľ nalákaný na špeciálne pripravenú webovú stránku. Iná možnosť je umiestniť ovládací prvok ActiveX označený ako „bezpečný na inicializáciu“ do aplikácie alebo dokumentu Microsoft Office, ktorý obsahuje renderovací engine IE.

Kritické zraniteľnosti CVE-2017-11813 a CVE-2017-11822 sú zapríčinené nesprávnym prístupom prehliadačmi Internet Explorer k objektom v pamäti. Pre úspešné zneužitie týchto zraniteľností musí byť užívateľ nalákaný na špeciálne pripravenú webovú stránku.

Pri všetkých uvedených zraniteľnostiach platí, že môžu zapríčiniť narušenie integrity pamäte, a tým umožniť útočníkovi na diaľku vykonať škodlivý kód. Útočník ďalej môže získať práva práve prihláseného používateľa. Ak je používateľ prihlásený ako správca, útočník môže prebrať kontrolu nad napadnutým systémom a následne inštalovať programy, prehliadať, meniť a zmazať dáta, a vytvárať nové užívateľské kontá s právomocami práve prihláseného používateľa.

Zraniteľné systémy:
Microsoft Internet Explorer 11 v systémoch Windows 7 for x64-based and 32-bit Systems Service Pack 1
Microsoft Internet Explorer 11 v systémoch Windows 8.1 for x64-based and 32-bit Systems
Microsoft Internet Explorer 11 v systéme Windows RT 8.1
Microsoft Internet Explorer 11 v systémoch Windows 10 verzií 1511, 1607 a 1703 v 32-bitových aj 64-bitových verziách
Microsoft Internet Explorer 11 v systémoch Windows 10 for x64-based and 32-bit Systems

Odporúčania:
Hoci nie je známy výskyt verejne dostupných exploitov, spoločnosť Microsoft pri všetkých 4 vyššie uvedených zraniteľnostiach uvádza, že ich zneužívanie je pravdepodobné. Preto odporúčame čím skôr 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-2017-11793
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11810
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11813
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11822

Microsoft Edge

V rámci októbrového balíka aktualizácií boli vydané opravy 19 kritických zraniteľností v prehliadači Microsoft Edge. Všetky z týchto kritických zraniteľností môžu spôsobiť narušenie integrity pamäte tak, že umožnia útočníkovi na diaľku vykonať škodlivý kód.

Kritické zraniteľnosti CVE-2017-11796, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11792, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11811, CVE-2017-11812 a CVE-2017-11821 sú dôsledkom spôsobu, akým skriptovací engine Chakra v prehliadačoch Edge spavuje objekty v pamäti. Pre úspešné zneužitie týchto zraniteľností musí byť užívateľ nalákaný webovú stránku so na špeciálne pripraveným obsahom. Pre zraniteľnosti CVE-2017-11799 a CVE-2017-11802 existujú verejne dostupné exploity.

Kritická zraniteľnosť CVE-2017-11809 spočíva v spôsobe spravovania objektov v pamäti skriptovacím engine-om Chakra v prehliadačoch od spoločnosti Microsoft. Pre úspešné zneužitie zraniteľností musí byť užívateľ nalákaný na webovú stránku so špeciálne pripraveným obsahom. Iná možnosť je umiestniť ovládací prvok ActiveX označený ako „bezpečný na inicializáciu“ do aplikácie alebo dokumentu Microsoft Office, ktorý obsahuje renderovací engine IE. Pre túto zraniteľnosť existuje verejne dostupný exploit.

Pri všetkých uvedených zraniteľnostiach platí, že môžu zapríčiniť narušenie integrity pamäte, a tým umožniť útočníkovi na diaľku vykonať škodlivý kód. Útočník ďalej môže získať práva práve prihláseného používateľa. Ak je používateľ prihlásený ako správca, útočník môže prebrať kontrolu nad napadnutým systémom a následne inštalovať programy, prehliadať, meniť a zmazať dáta, a vytvárať nové užívateľské kontá s právomocami práve prihláseného používateľa.

Zraniteľné systémy:
Microsoft Edge v systémoch Windows 10 verzií 1511, 1607 a 1703 v 32-bitových aj 64-bitových verziách
Microsoft Edge v systémoch Windows 10 for x64-based and 32-bit Systems

Odporúčania:
Vzhľadom na výskyt verejne dostupných exploitov 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-2017-11796
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11798
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11799
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11800
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11792
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11802
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11804
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11805
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11806
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11807
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11808
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11809
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11811
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11812
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11821

Mozilla Firefox

Spoločnosť Mozilla v októbri nevydala opravy žiadnych zraniteľností v prehliadači Firefox.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/mfsa2017-23/

Google Chrome

Spoločnosť Google v októbri vydala dve aktualizácie pre prehliadač Chrome. V rámci prvej aktualizácie bolo opravených dokopy 35 zraniteľností. Zo 20 zverejnených opráv nie je ani jedna kritická a 8 je dôležitých.

V rámci druhej aktualizácie bola opravená 1 kritická zraniteľnosť, CVE-2017-15396, objavená vo voľne dostupnom V8 JavaScript engine používanom v prehliadačoch Google Chrome. Chyba spočíva možnosti spôsobiť pretečenie zásobníka, čo sa následne dá využiť na vykonanie škodlivého kódu.

V čase písania tohto mesačníka (6.11.) pribudla nová verzia prehliadača Chrome, v ktorej bola opravená 1 kritická zraniteľnosť v protokole QUIC umožňujúca spôsobiť pretečenie zásobníka.

Zraniteľné systémy:
Google Chrome 62.0.3202.75 a staršie

Odporúčania:
Odporúčame overiť, či sa prehliadač Chrome automaticky aktualizoval na najnovšiu verziu 62.0.3202.89. Ak aktualizácia neprebehla automaticky, odporúčame aplikovať aktualizáciu manuálne – otvorením okna s aktuálne nainštalovanou verziou cez menu, čo zároveň spustí kontrolu dostupnosti aktualizácie.

Zdroje:
https://chromereleases.googleblog.com/2017/
https://chromereleases.googleblog.com/2017/10/stable-channel-update-for-desktop_26.html
https://chromereleases.googleblog.com/2017/10/stable-channel-update-for-desktop.html

4. Adobe

Adobe Flash Player

Spoločnosť Adobe vydala v októbri opravu jednej kritickej zraniteľnosti v aplikácii Adobe Flash Player. Ide o zraniteľnosť CVE-2017-11292, ktorá umožňuje zámenu typu objektov a jej zneužitie môže viesť k vzdialenému vykonaniu škodlivého kódu. Na zneužitie je potrebné, aby používateľ otvoril špeciálne pripravený súbor, umiestnený napríklad na webovej stránke alebo v prílohe emailu.

Zraniteľné systémy:
Adobe Flash Player Desktop Runtime 27.0.0.159 a staršie (Windows, Macintosh a Linux)
Adobe Flash Player for Google Chrome 27.0.0.159 a staršie (Windows, Macintosh, Linux a Chrome OS)
Adobe Flash Player for Microsoft Edge and Internet Explorer 11 27.0.0.159 a staršie (Windows 10 a 8.1)

Odporúčania:
Vzhľadom na fakt, že existujú správy o zneužívaní tejto zraniteľnosti, 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/apsb17-32.html
https://securitytracker.com/id/1039582
https://threatpost.com/adobe-patches-flash-zero-day-exploited-by-black-oasis-apt/128467/
https://thehackernews.com/2017/10/flash-player-zero-day.html
https://get.adobe.com/flashplayer/

5. Frameworky

Microsoft .NET

V rámci októbrového balíka aktualizácií spoločnosť Microsoft nevydala žiadne opravy zraniteľností vo frameworkoch .NET.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/313ae481-3088-e711-80e2-000d3a32fc99
https://portal.msrc.microsoft.com/en-us/security-guidance

Oracle Java SE

Spoločnosť Oracle v mesiaci október vydala opravy 32 zraniteľností, z ktorých 28 môže byť zneužitých vzdialene bez nutnosti autentifikácie. Počet kritických zraniteľností je 10, pričom všetky sú zneužiteľné cez internetovú sieť bez nutnosti autentifikácie.

Prvých 9 kritických zraniteľností vyžaduje pre úspešné zneužitie interakciu používateľa. Ak používateľ nie je prihlásený s právomocami administrátora, závažnosť týchto zraniteľností je výrazne nižšia, čím prestávajú byť kritickými. Zároveň sa tieto zraniteľnosti týkajú inštalácií Javy, ktoré načítavajú a spúšťajú nedôveryhodný kód, napr. z internetu, a ohľadom bezpečnosti sa spoliehajú na Java sandbox mechanizmus. Naopak, zraniteľnosti sa netýkajú inštalácií, typicky na serveroch, ktoré spúšťajú len dôveryhodný kód, napr. nainštalovaný správcom. Zraniteľnosť CVE-2017-10110 je spôsobená chybou v komponente AWT pre vytváranie grafického rozhrania, zraniteľnosť CVE-2017-10089 chybou v triede ImageIO, CVE-2017-10086 je spôsobená chybou v komponente JavaFX, zraniteľnosti CVE-2017-10096 a CVE-2017-10101 sú zapríčinené chybou v komponente JAXP, zraniteľnosti CVE-2017-10087, CVE-2017-10090 a CVE-2017-10111sú spôsobené chybou v komponente Libraries, a zraniteľnosť CVE-2017-10107 zapríčiňuje chyba v komponente RMI pre vzdialené volanie metód. Tieto zraniteľnosti sú jednoducho zneužiteľné cez internetovú sieť prostredníctvom viacerých protokolov. Ich zneužitím môže útočník prevziať kontrolu nad Java SE a/alebo Java SE Embedded. Pritom je zároveň potrebné, aby užívateľ umožnil otvorenie škodlivého obsahu buď priamo otvorením špeciálne pripraveného súboru alebo navštívením webovej stránky so škodlivým obsahom.

Kritická zraniteľnosť CVE-2017-10102 je tiež spôsobená chybou v komponente RMI. Jej zneužitie je komplikované, avšak nevyžaduje žiadnu akciu od používateľa. Prostredníctvom internetovej siete je možné cez viacero protokolov poškodiť a prevziať kontrolu nad produktami Java SE a Java SE Embedded. Zneužiť túto zraniteľnosť je možné jedine poskytnutím špeciálnych dát do programovacieho rozhrania RMI, a to bez využitia nedôveryhodných Java Web Start aplikácií alebo nedôveryhodných Java appletov.

Pre zraniteľnosť CVE-2017-10309, označenú ako dôležitá, existuje verejne dostupný exploit. Táto zraniteľnosť je zneužiteľná cez internetovú sieť prostredníctvom viacerých protokolov. Úspešné zneužitie si vyžaduje interakciu používateľa a môže viesť k neoprávnenej zmene, pridaniu alebo zrušeniu prístupu k niektorým dátam prístupným prostredníctvom Java SE. Ďalej môže zneužitie tejto zraniteľnosti viesť k neoprávnenému čítaniu dát prístupných cez Java SE, spôsobeniu čiastočnej nedostupnosti servisu (DoS) Java SE. Táto zraniteľnosť sa týka inštalácií Javy, ktoré načítavajú a spúšťajú nedôveryhodný kód, napr. z internetu, a ohľadom bezpečnosti sa spoliehajú na Java sandbox mechanizmus. Naopak, zraniteľnosť sa netýkaj inštalácií, typicky na serveroch, ktoré spúšťajú len dôveryhodný kód, napr. nainštalovaný správcom.

Zraniteľné systémy:
Oracle Java SE: 6u151, 7u141, 8u151 a staršie
Oracle Java SE Embedded: 8u131 a staršie

Odporúčania:
Vzhľadom na závažnosť uvedených zraniteľností a výskyt verejne dostupného exploitu, odporúčame čo najskôr aktualizovať zraniteľné verzie Java SE a Java SE Embedded na aktuálne verzie, t.j. Java SE 6u171, Java SE 7u161, Java SE 8u152, Java SE Embedded 8u151, prostredníctvom Java Auto Update, alebo na stránke spoločnosti Oracle, viď prvý odkaz v zdrojoch.

Zdroje:
http://www.oracle.com/technetwork/indexes/downloads/index.html#java
http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
https://nvd.nist.gov/vuln/detail/CVE-2017-10110
https://nvd.nist.gov/vuln/detail/CVE-2017-10089
https://nvd.nist.gov/vuln/detail/CVE-2017-10086

https://nvd.nist.gov/vuln/detail/CVE-2017-10096
https://nvd.nist.gov/vuln/detail/CVE-2017-10101
https://nvd.nist.gov/vuln/detail/CVE-2017-10087
https://nvd.nist.gov/vuln/detail/CVE-2017-10090
https://nvd.nist.gov/vuln/detail/CVE-2017-10111
https://nvd.nist.gov/vuln/detail/CVE-2017-10107
https://nvd.nist.gov/vuln/detail/CVE-2017-10102
https://nvd.nist.gov/vuln/detail/CVE-2017-10309
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10309

6. Iné závažné zraniteľnosti

Kritická zraniteľnosť vo firmvéri TPM modulov

Koncom októbra bola zverejnená informácia o kritickej zraniteľnosti CVE-2017-15361 vo firmvéri modulov TPM (Trusted Platform Module) od spoločnosti Infineon. TPM modul je voliteľný hardvérový bezpečnostný prvok, ktorý zariadeniam poskytuje viaceré bezpečnostné a kryptografické funkcie ako napríklad generovanie, skladovanie a správa kryptografických kľúčov, autentifikácia a ochrana zariadenia pred zásahmi zvonka. Zraniteľnosť spočíva v chybe pri generovaní RSA kľúča, kedy nie je skutočne zaistená náhodnosť generovaných hodnôt. Kvôli tomu je pre útočníkov technicky možné prelomiť kľúč, a teda získať privátny kľúč faktorizáciou verejného. Útok je dosiahnuteľný pre bežne používané dĺžky kľúčov, vrátane 1024- a 2048-bitových kľúčov – hoci faktorizácia môže trvať aj dlhší ča. K útoku stačí získať verejný kľúč. Ku dňu písania tohto mesačníka nebolo zaznamenané zneužitie tejto zraniteľnosti. V súčasnej dobe výrobcovia TPM modulov vydávajú aktualizácie s opravami TPM firmvérov.

Zraniteľné hardvérové moduly:

TPM moduly s verziami firmvéru (môžu byť aj ďalšie):
staršie ako 0000000000000422 - 4.34
staršie ako 000000000000062b - 6.43
staršie ako 0000000000008521 - 133.33

Zraniteľné systémy Microsoft Windows:

Windows 10 32- aj 64-bitové verzie
Windows 10 verzie 1511 v 32- aj 64-bitové verzie
Windows 10 verzie 1607 v 32- aj 64-bitové verzie
Windows 10 verzie 1703 v 32- aj 64-bitové verzie
Windows 8.1 32 aj 64-bitové verzie
Windows RT 8.1
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016

Niektoré ďalšie zasiahnuté softvérové produkty:

Bitlocker s TPM 1.2
YubiKey verzie staršie ako 4.3.5
Chrome OS

Odporúčania:

Spoločnosť Microsoft vydala pre svoje operačné systémy bezpečnostnú aktualizáciu, ktorá dočasne nahradí generovanie RSA kľúčov bezpečnejšími softvérovými funkciami, a ktorú odporúčame čo najskôr aplikovať. Aktualizácia zároveň obsahuje funkcie, ktoré uľahčia správcom identifikovať zraniteľné zariadenia v ich sieťach. Podrobnosti sú uvedené na prvom odkaze v referenciách. Až následne odporúčame aplikovať aktualizáciu pre TPM modul, ak už je k dispozícii. Ďalšie kroky aj s podrobnejším popisom možno taktiež nájsť na prvom odkaze.

Zdroje:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV170012
https://www.infineon.com/cms/en/product/promopages/tpm-update/?redirId=59160
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15361
https://threatpost.com/factorization-flaw-in-tpm-chips-makes-attacks-on-rsa-private-keys-feasible/128474/