Mesačný prehľad kritických zraniteľností

Júl 2017

1. Operačné systémy Microsoft Windows

V mesiaci júli vydala spoločnosť Microsoft opravu kritickej zraniteľnosti CVE-2017-8463 vo Windows Exploreri, ktorá útočníkovi umožňuje na diaľku vykonať škodlivý kód s právomocami práve prihláseného používateľa. Pre úspešné zneužitie musí útočník vytvoriť a zdieľať zdieľaný priečinok a škodlivý vykonateľný súbor a následne presvedčiť používateľa, že zdieľaný škodlivý vykonateľný súbor je tiež iba zdieľaný priečinok.

Bola opravená kritická zraniteľnosť CVE-2017-8584 v Microsoft HoloLens, ktorá útočníkovi umožňuje zneužiť chybu v narábaní s objektami v pamäti zaslaním špeciálne pripraveného wifi paketu, v dôsledku čoho môže útočník získať plnú kontrolu nad zariadením.

Ďalšia vydaná oprava sa týka kritickej zraniteľnosti CVE-2017-8589 vo Windows Search, ktorá spočíva v chybe pri narábaní s objektmi v pamäti. Pri úspešnom zneužití zraniteľnosti môže útočník získať plnú kontrolu nad zariadením, a to podsunutím špeciálne vytvoreného vstupu, buď lokálne alebo na diaľku cez protokol SMB.

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:

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-2017-8463
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8584

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft v rámci júlového balíka aktualizácií nevydala pre softvérovú sadu Office žiadne opravy kritických zraniteľností, avšak boli vydané opravy ôsmich zraniteľností – označených ako dôležité. Sú to zraniteľnosti CVE-2017-0243, CVE-2017-8501, CVE-2017-8502 a CVE-2017-8570. Útočníkom môžu byť zneužité na vzdialené vykonanie škodlivého kódu spôsobením narušenia integrity pamäte pomocou špeciálne pripraveného súboru, dopraveného na cieľové zariadenie emailom alebo cez webovú stránku. Pre úspešné zneužitie týchto zraniteľností je nevyhnutná interakcia používateľa.

V mesiaci júli bola vydaná dôležitá oprava zraniteľnosti CVE-2017-8571 v softvéri Microsoft Outlook, ktorá umožňuje útočníkovi zneužiť chybu pri spracovaní vstupu. Pomocou špeciálne pripraveného súboru je možné obísť bezpečnostné prvky softvéru a následne vykonávať na cieľovom zariadení ľubovoľné príkazy. Pre úspešné zneužitie je potrebná interakcia používateľa.

Ďalšia oprava sa týka zraniteľnosti CVE-2017-8572 softvéri Microsoft Outlook, označenej ako dôležitá. Útočník môže pomocou pripravenej webovej stránky zneužiť chybu pri spracovaní výsledkov autentifikácie, čo môže mať za následok získanie NTLM hashu útočníkom po tom, ako používateľ túto stránku navštívi. Druhou možnosťou je podstrčenie špeciálne pripraveného súboru, po otvorení ktorého sa inicializuje pokus o NTLM autentifikáciu. Útočník by následne mohol za účelom získania prihlasovacieho hesla pokúsiť o prelomenie získaného hashu.

Opravená zraniteľnosť CVE-2017-8663 v softvéri Microsoft Outlook bola označená ako dôležitá. Pre zneužitie môže útočník používateľovi prostredníctvom emailovej správy podstrčiť špeciálne pripravený súbor. Ak ho používateľ otvorí, dôjde ku narušeniu integrity pamäte, v dôsledku čoho útočník získa plnú kontrolu nad cieľovým zariadením.

Ďalšou júlovou opravou je oprava dôležitej zraniteľnosti CVE-2017-8569 v softvéri SharePoint Server, ktorá autentifikovanému útočníkovi umožňuje povýšenie právomocí zaslaním špeciálne pripraveného webového paketu. Útočník tým získa možnosť vykonania XSS útoku, výsledkom ktorého môže byť únik dát alebo ukradnutie identity poškodeného používateľa, čo môže útočník ďalej zneužiť na získanie kontroly nad SharePoint lokalitou.

Zraniteľné systémy:

Microsoft Office 2010 Click-to-Run (C2R) for 32-bit editions
Microsoft Office 2010 Click-to-Run (C2R) for 64-bit editions
Microsoft Office 2013 Click-to-Run (C2R) for 32-bit editions
Microsoft Office 2013 Click-to-Run (C2R) for 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 2007 Service Pack 3
Microsoft Outlook 2010 Service Pack 2 (32-bit editions)
Microsoft Outlook 2010 Service Pack 2 (64-bit editions)
Microsoft Outlook 2013 RT Service Pack 1
Microsoft Outlook 2013 Service Pack 1 (32-bit editions)
Microsoft Outlook 2013 Service Pack 1 (64-bit editions)
Microsoft Outlook 2016 (32-bit edition)
Microsoft Outlook 2016 (64-bit edition)
Microsoft Business Productivity Servers 2010 Service Pack 2
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 Excel 2007 Service Pack 3
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 2007 Service Pack 3
Microsoft Office Compatibility Pack Service Pack 3
Microsoft Office Online Server 2016
Microsoft SharePoint Enterprise Server 2013
Microsoft SharePoint Enterprise Server 2016

Odporúčania:

Odporúčame čo najskôr aplikovať aktualizácie publikované prostredníctvom služby Windows Update, nakoľko sa s veľkou pravdepodobnosťou môžu vyskytnúť verejne dostupné exploity na tento typ zraniteľností. 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-2017-8571
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8572
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8663
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0243
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8501
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8502
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8569
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8570

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft v júli vydala opravu kritickej zraniteľnosti CVE-2017-8594, zneužitím ktorej útočník získa možnosť vzdialeného vykonania škodlivého kódu s právomocami práve prihláseného používateľa. Pre úspešné zneužitie musí útočník pripraviť špeciálnu webovú stránku, prípadne škodlivý obsah, a následne nalákať používateľa na navštívenie danej stránky – napríklad prostredníctvom emailovej správy. Na túto zraniteľnosť je verejne dostupný exploit.

V rámci júlového balíka opráv boli spoločnosťou Microsoft vydané opravy kritických zraniteľností v JavaScript engine, CVE-2017-8606, CVE-2017-8607 a CVE-2017-8608. Tieto zraniteľnosti umožňujú útočníkovi 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, otvorením ktorého rovnako dôjde k zneužitiu zraniteľnosti.

Bola opravená kritická zraniteľnosť CVE-2017-8618 vo VBScript engine, ktorá spočíva v chybe pri narábaní s objektami 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 alebo škodlivý webový obsah a nalákať používateľa na navštívenie danej stránky. Druhou možnosťou je umiestnenie škodlivého JavaScript obsahu do Microsoft Office dokumentu, otvorením ktorého rovnako dôjde k zneužitiu zraniteľnosti.

Zraniteľné systémy:
Microsoft Internet Explorer 9
Microsoft Internet Explorer 10
Microsoft Internet Explorer 11

Odporúčania:
Vzhľadom na výskyt verejne dostupného exploitu na jednu z uvedených zraniteľností, 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-2017-8594
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8606
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8618

Microsoft Edge

V júli bola vydaná oprava kritickej zraniteľnosti CVE-2017-8518. Chyba spočíva v prístupe k objektom v pamäti, čo môže útočník zneužiť na spôsobenie narušenia integrity pamäte, čím získa možnosť na diaľku vykonať škodlivý kód. 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.

Spoločnosť Microsoft v júli vydala pre prehliadač Edge opravy kritických zraniteľností CVE-2017-8595, CVE-2017-8596, CVE-2017-8598, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8609, CVE-2017-8610, CVE-2017-8617 a CVE-2017-8619. Menované zraniteľnosti 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 sú umiestnenie škodlivého obsahu na webovú stránku s používateľským obsahom, prípadne umiestnenie tohto obsahu do Microsoft Office dokumentu, otvorením ktorého rovnako dôjde k zneužitiu zraniteľnosti.

V rámci júlového balíka aktualizácií boli vydané opravy pre ďalšie kritické zraniteľnosti v JavaScript engine, CVE-2017-8601, CVE-2017-8606, CVE-2017-8607 a CVE-2017-8608. Útočník môže zneužiť chybu v narábaní s objektami v pamäti a tým získať možnosť na diaľku vykonať 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 sú umiestnenie škodlivého obsahu na webovú stránku s používateľským obsahom, prípadne umiestnenie tohto obsahu do Microsoft Office dokumentu, otvorením ktorého rovnako dôjde k 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:
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-2017-8518
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8595
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8601

Mozilla Firefox

Spoločnosť Mozilla v júli pre prehliadač Firefox nevydala žiadne aktualizácie.

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

Google Chrome

Spoločnosť Google v júli vydala aktualizáciu pre prehliadač Chrome, obsahujúcu opravu 40 zraniteľností. Kritická zraniteľnosť CVE-2017-5091 v komponente IndexedDB spočíva v použití už predtým uvoľnenej pamäte, čo môže mať za následok možnosť pre útočníka vykonať na diaľku škodlivý kód.

Ďalej v júlovej aktualizácii boli opravené kritické zraniteľností CVE-2017-5092 a CVE-2017-5099 komponente PPAPI, ktoré spočívajú v použití uvoľnenej pamäte a v zápise mimo pridelenú pamäť, čo môže útočník zneužiť na vzdialené vykonanie škodlivého kódu.

Opravená kritická zraniteľnosť CVE-2017-5093 vo webovom engine Blink umožňuje útočníkovi vykonať útok s predstieraním falošného používateľského rozhrania s bližšie nešpecifikovanými následkami.

Kritická zraniteľnosť CVE-2017-5095 v komponente PDFium, opravená v rámci júlových aktualizácií, spočíva v zápise mimo pridelenú pamäť, čo má pravdepodobne za následok možnosť pre útočníka vykonať na diaľku škodlivý kód.

Bola vydaná oprava kritickej zraniteľnosti CVE-2017-5097 v grafickej knižnici Skia, ktorá spočíva v zápise mimo pridelený rozsah pamäte. Možné následky prípadného zneužitia neboli bližšie špecifikované.

Spoločnosť Google vydala v júli opravu kritickej zraniteľnosti CVE-2017-5098 v komponente V8 (open-source JavaScript engine), ktorá spočíva v použití už predtým uvoľnenej pamäte, čo má pravdepodobne za následok možnosť pre útočníka vykonať na diaľku škodlivý kód.

Zraniteľné systémy:
Google Chrome 59.0.3071.115 a staršie

Odporúčania:
Odporúčame overiť, či sa prehliadač Chrome automaticky aktualizoval na najnovšiu verziu 60.0.3112.78, prípadne novšiu. V prípade potreby odporúčame aplikovať aktualizáciu manuálne cez menu, a to otvorením okna s aktuálne nainštalovanou verziou, čo zároveň spustí kontrolu dostupnosti aktualizácie.

Zdroje:
https://chromereleases.googleblog.com/2017/07/stable-channel-update-for-desktop.html

4. Adobe

Adobe Flash Player

Spoločnosť Adobe vydala v mesiaci júl opravy troch zraniteľností v aplikáciách Adobe Flash Player. Kritická je zraniteľnosť CVE-2017-3099, ktorá po načítaní špeciálne pripraveného obsahu spôsobí narušenie integrity pamäte a umožní vykonanie škodlivého kódu. Ďalšie dve opravené zraniteľnosti sú klasifikované ako dôležité, pre ich zneužitie je tiež potrebné načítanie špeciálne pripraveného obsahu. Zneužitím CVE-2017-3080 je možné obísť bezpečnostné obmedzenia a môže dôjsť k úniku potenciálne citlivých informácií. Zraniteľnosť CVE-2017-3100 umožňuje narušenie integrity pamäte a únik adresy pamäte s potenciálne citlivými informáciami. Na žiadnu zo zraniteľností nie je známy verejne dostupný exploit.

Zraniteľné systémy:
Adobe Flash Player Desktop Runtime 26.0.0.131 a staršie (Windows, Macintosh and Linux)
Adobe Flash Player for Google Chrome 26.0.0.131 a staršie (Windows, Macintosh, Linux and Chrome OS)
Adobe Flash Player for Microsoft Edge and Internet Explorer 11 26.0.0.120 (Windows 10 and 8.1)
Adobe Flash Player Desktop Runtime verzie staršie ako 26.0.0.137 (Linux)

Odporúčania:
Odporúčame aktualizovať Flash Player na verziu 26.0.0. V závislosti od prehliadača a nastavení používateľa sa aktualizácia udeje 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/apsb17-21.html
https://threatpost.com/adobe-fixes-six-vulnerabilities-in-flash-connect-with-july-update/126747/
https://get.adobe.com/flashplayer/

5. Frameworky

Microsoft .NET

V rámci júlového balíka aktualizácií vydala spoločnosť Microsoft opravu zraniteľnosti CVE-2017-8585, označenej ako dôležitá. Spočíva v chybe v knižnici Microsoft Common Object Runtime Library (mscorlib) pri spracovaní webových žiadostí. Neautentifikovaný útočník môže na diaľku spôsobiť zrútenie aplikácie špeciálne pripravenou webovou žiadosťou.

Zraniteľné systémy:
Microsoft .NET Framework 4.6
Microsoft .NET Framework 4.6.1
Microsoft .NET Framework 4.6.2
Microsoft .NET Framework 4.7

Odporúčania:
Odporúčame aplikovať aktualizácie, publikované prostredníctvom služby Windows Update.

Zdroje:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8585

Oracle Java SE

Spoločnosť Oracle v júli vydala balík aktualizácií s 310 opravami zraniteľností. Popis zraniteľností a zoznam všetkých produktov, ktorých sa tieto opravy týkajú je možné nájsť na prvom odkaze v sekcii zdroje.

Aktualizácia produktov Oracle Java SE obsahuje opravy 32 zraniteľností, z ktorých 10 je kritických a 11 dôležitých. 28 zraniteľností je zneužiteľných vzdialene bez nutnosti autentifikácie. Všetky kritické zraniteľnosti vyžadujú pre úspešné zneužitie interakciu používateľa.

Väčšina zraniteľností (9 z 10 kritických: CVE-2017-10110, CVE-2017-10089, CVE-2017-10086, CVE-2017-10096, CVE-2017-10101, CVE-2017-10087, CVE-2017-10090, CVE-2017-10111, CVE-2017-10107) sa týka inštalácií, ktoré môžu načítať nedôveryhodný kód, napr. z internetu. Typicky ide o Java Web Start alebo Java applety bežiace v izolovanom priestore (tzv. sandbox), ktoré sa spoliehajú na bezpečnosť takéhoto izolovaného priestoru. Tieto zraniteľnosti sa netýkajú inštalácií Javy, najmä na serveroch, ktoré načítavajú len dôveryhodný kód, napr. nainštalovaný administrátorom. Úspešným zneužitím menovaných zraniteľností môže útočník získať povýšenie právomocí a pravdepodobne možnosť pokračovať ďalej v útoku. Na žiadnu zo zraniteľností nie je momentálne známy verejne dostupný exploit.

Zraniteľné systémy:

Oracle Java SE 6u151 a staršie
Oracle Java SE 7u141 a staršie
Oracle Java SE 8u131 a staršie
Oracle Java SE Embedded 8u131 a staršie

Odporúčania:

Odporúčame aktualizácie zraniteľné verzie Javy SE na aktuálne verzie, t.j. Java SE 6u161, Java SE 7u151, Java SE 8u144, Java SE Embedded 8u144, prostredníctvom Java Auto Update, alebo na stránke spoločnosti Oracle, viď posledný odkaz v zdrojoch.

Zdroje:

http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
http://www.securitytracker.com/id/1038931
https://nvd.nist.gov/vuln/detail/CVE-2017-10110
http://www.oracle.com/technetwork/indexes/downloads/index.html#java

6. Iné závažné zraniteľnosti

Kritická zraniteľnosť vo firmvéri Broadcom WiFi čipovej súpravy.

Koncom júla bol zverejnený dôkaz existencie exploitu na kritickú zraniteľnosť vo firmvéroch WiFi čipových sád od spoločnosti Broadcom, ktorá útočníkovi umožňuje spustiť masívny červovitý útok na zariadenia so zraniteľnými čipmi. Útočníkove zariadenie môže vysielať špeciálne pripravené WiFi pakety všetkým zariadeniam v okolí. Zraniteľnosť spočíva vo fakte, že špeciálne pripraveným WiFi paketom je možné spôsobiť prepísanie firmvéru WiFi čipu tak, že napadnuté zariadenie začne vysielať rovnaké škodlivé pakety. Pre úspešné zneužitie používateľ nemusí byť pripojený na rovnakej WiFi sieti ako útočník, úplne postačuje, že je na zariadení zapnutý WiFi prijímač. Po napadnutí firmvéru WiFi čipovej súpravy má útočník možnosť pokračovať v útoku na ďalšie súčasti zariadenia. Spoločnosti Google a Apple už začiatkom júla vydali na túto zraniteľnosť opravy, dovtedy bola podľa odhadov až miliarda zraniteľných zariadení. Laptopy a stolové počítače pravdepodobne nie sú zraniteľné vďaka odlišnej hardvérovej štruktúre.

Zraniteľné systémy:

Zraniteľnosť bola demonštrovaná na zariadeniach s Broadcom čipmi:
Samsung Galaxy
Nexus
iPhone

Odporúčania:

Najspoľahlivejším spôsobom ochrany je čo najskoršia aplikácia aktualizácií publikovanými výrobcom daného zariadenia, resp. mobilného operačného systému.

Zdroje:

https://arstechnica.com/information-technology/2017/07/broadcom-chip-bug-opened-1-billion-phones-to-a-wi-fi-hopping-worm-attack/