Mesačný prehľad kritických zraniteľností

August 2017

1. Operačné systémy Microsoft Windows

V auguste vydala spoločnosť Microsoft opravu kritickej zraniteľnosti CVE-2017-8620 vo Windows Search, ktorá spočíva v spôsobe narábania s objektami v pamäti. Pre úspešné zneužitie musí útočník poslať službe Windows Search špeciálne pripravené správy. Lokálny útočník by mohol zneužiť túto zraniteľnosť na povýšenie právomocí a prevzatie plnej kontroly nad zariadením. Oveľa závažnejší je fakt, že túto zraniteľnosť môže zneužiť aj vzdialený útočník cez pripojenie SMB, s rovnakými dôsledkami.

Kritická zraniteľnosť CVE-2017-0250 v Microsoft JET Database Engine umožňuje útočníkovi, zneužitím chyby pri narábaní s pamäťou, na diaľku získať potenciálne plnú kontrolu nad zariadením. Používateľské účty s menšími právomocami môžu byť zasiahnuté menej. Pre úspešné zneužitie musí používateľ otvoriť špeciálne pripravený databázový súbor, ktorý mu bol útočníkom zaslaný napríklad cez email, pričom daný súbor stačí otvoriť v paneli náhľadu.

Kritická zraniteľnosť CVE-2017-0293 vo Windows PDF umožňuje útočníkovi zneužiť chybu v narábaní s pamäťou, v dôsledku čoho môže získať možnosť vykonania škodlivého kódu s právomocami práve prihláseného používateľa. Pre úspešné zneužitie zraniteľnosti musí používateľ otvoriť špeciálne pripravený PDF súbor so škodlivým obsahom, ktorý mu bol dopravený napríklad prostredníctvom emailu. Avšak, v prípade použitia prehliadača Microsoft Edge na operačnom systéme Windows 10, dochádza ku zneužitiu zraniteľnosti už pri zobrazení PDF súboru v prehliadači. V tom prípade útočníkovi stačí pripraviť webovú stránku so škodlivým súborom, prípadne ho umiestniť na stránku so zdieľaným používateľským obsahom.

Ďalšia vydaná oprava sa týka kritickej zraniteľnosti CVE-2017-8591 vo Windows Input Method Editor, ktorá spočíva v chybe pri spracovaní argumentov funkcie v rámci triedy DCOM. Pre úspešné zneužitie musí lokálne autentifikovaný útočník spustiť špeciálne pripravenú aplikáciu, čím získa možnosť ďalšieho vykonávania škodlivého kódu.

Kritická zraniteľnosť CVE-2017-8622 vo Windows Subsystem for Linux, ktorá spočíva v spôsobe narábania s NT presmerovaniami (NT pipes). Pre úspešné zneužitie musí lokálne autentifikovaný útočník spustiť špeciálne pripravenú aplikáciu, dôsledkom čoho získa povýšené právomoci.

Za zmienku stojí tiež vydanie opravy zraniteľnosti CVE-2017-8664, označenej ako dôležitá, v komponente Hyper-V. Zraniteľnosť spočíva v chybe pri spracovaní vstupu od autentifikovaného používateľa, prihláseného na hosťovskom systéme. Pre zneužitie zraniteľnosti je potrebné na hosťovskom systéme spustiť špeciálne pripravenú aplikáciu, ktorá môže zapríčiniť vykonanie ľubovoľného kódu na hostiteľskom systéme.

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:
Vzhľadom na zvýšenú pravdepodobnosť zneužitia niektorých 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, a to 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-2017-8620
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0250
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0293
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8591
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8622
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8664

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft v rámci augustového balíka aktualizácií nevydala pre softvérovú sadu Office žiadne opravy kritických zraniteľností, avšak bola vydaná oprava zraniteľnosti CVE-2017-8654, označenej ako dôležitá. Autentifikovaný útočník môže zneužiť chybu v Microsoft SharePoint Server pri spracovaní webových požiadaviek. Zaslaním špeciálne pripravenej požiadavky môže útočník získať možnosť vykonania XSS útoku na napadnutom systéme a vykonávať kód s právomocami práve prihláseného používateľa, prípadne pristupovať k dátam, zaujať identitu používateľa alebo umiestniť na server škodlivý obsah.

Zraniteľné systémy:
Microsoft SharePoint Enterprise Server 2010 Service Pack 2

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-2017-8654

3. Internetové prehliadače

Microsoft Internet Explorer

V rámci augustového balíka opráv boli spoločnosťou Microsoft vydané opravy kritických zraniteľností CVE-2017-8635, CVE-2017-8636 a CVE-2017-8641 v JavaScript engine, ktoré útočníkovi umožňujú 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 dôjde ku zneužitiu týchto zraniteľností.

V auguste vydaná oprava kritickej zraniteľnosti CVE-2017-8653 spočíva v chybnom prístupe k objektom 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 stránku so zdieľaným používateľským obsahom, a následne nalákať používateľa na navštívenie danej stránky – napríklad prostredníctvom emailovej správy.

Spoločnosť Microsoft v auguste vydala opravu kritickej zraniteľnosti CVE-2017-8669 spočívajúcej v chybe pri narábaní s objektami v pamäti. Útočník môže spôsobením narušenia integrity pamäte získať možnosť vykonania škodlivého kódu. Pre úspešné zneužitie potrebuje útočník pripraviť špeciálnu webovú stránku alebo škodlivý webový obsah a nalákať používateľa na navštívenie danej stránky. Druhou možnosťou je umiestnenie škodlivého obsahu do dokumentu Microsoft Office, otvorením ktorého rovnako dôjde ku zneužitiu zraniteľnosti.

Zraniteľné systémy:
Microsoft Internet Explorer 10
Microsoft Internet Explorer 11

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-2017-8635
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8641
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8636
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8653
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8669

Microsoft Edge

V rámci augustového balíka aktualizácií boli vydané opravy 21 kritických zraniteľností v prehliadači Edge. Sedemnásť z nich sú kritické zraniteľnosti CVE-2017-8634 až CVE-2017-8636, CVE-2017-8638 až CVE-2017-8641, CVE-2017-8645 až CVE-2017-8647, CVE-2017-8655 až CVE-2017-8657, CVE-2017-8670 až CVE-2017-8672 a CVE-2017-8674 v Chakra JavaScript Engine. Spočívajú v chybnom spôsobe narábania s objektami v pamäti. Útočník môže spôsobením narušenia integrity pamäte získať možnosť vzdialeného vykonania škodlivého kódu s právomocami práve prihláseného používateľa. Pre úspešné zneužitie musí používateľ navštíviť špeciálne pripravenú webovú stránku, respektíve stránku s umiestneným škodlivým obsahom. Druhou možnosťou je umiestnenie JavaScript obsahu do dokumentu Microsoft Office, otvorením ktorého rovnako dôjde ku zneužitiu týchto zraniteľností. Na jedenásť z menovaných zraniteľností sú verejne dostupné exploity.

Kritická zraniteľnosť CVE-2017-8653 spočíva v chybnom prístupe k objektom v pamäti. To môže útočník zneužiť na spôsobenie narušenia integrity pamäte, čím získa možnosť na diaľku vykonať škodlivý kód s právomocami práve prihláseného používateľa. 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.

Kritické zraniteľnosti CVE-2017-8661 a CVE-2017-8669 v prehliadači Edge 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 je umiestnenie škodlivého obsahu na webovú stránku so zdieľaným používateľským obsahom, prípadne umiestnenie tohto obsahu do dokumentu Microsoft Office, otvorením ktorého rovnako dôjde k zneužitiu zraniteľnosti.

V auguste bola vydaná oprava kritickej zraniteľnosti CVE-2017-8518 spočívajúca v nesprávnom prístupe k objektom v pamäti, čo môže útočník zneužiť na vykonanie škodlivého kódu s právomocami práve prihláseného používateľa. Útočník potrebuje vytvoriť škodlivú webstránku, prípadne umiestniť škodlivý obsah na stránku so zdieľaným používateľským obsahom. Pre úspešné zneužitie útočník potrebuje nalákať používateľa na návštevu pripravenej stránky, napríklad prostredníctvom emailovej správy alebo cez otvorenie škodlivej emailovej prílohy.

V rámci augustového balíka aktualizácií boli vydané opravy zraniteľností CVE-2017-8644 a CVE-2017-8652, označené ako dôležité, ktoré útočníkovi umožňujú zneužiť chybu v narábaní s objektami v pamäti, a tým spôsobiť únik informácií, ktoré môžu útočníkovi pomôcť v ďalšom pokračovaní útoku. Pre úspešné zneužitie potrebuje útočník pripraviť škodlivú webovú stránku a nalákať používateľa na navštívenie danej stránky. Inou možnosťou je umiestnenie škodlivého obsahu na webovú stránku s používateľským obsahom. Na obe menované zraniteľnosti sú verejne dostupné exploity.

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:
Vzhľadom na vysoký počet verejne dostupných exploitov 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-2017-8634
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8653
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8669
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8518
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8644

Mozilla Firefox

Spoločnosť Mozilla vydala v auguste opravy piatich kritických zraniteľností v prehliadači Firefox.

Zraniteľnosť CVE-2017-7798 spočíva v chybe spracovania zdrojového kódu webstránky pri jeho otvorení v editore štýlov. Útočník po vložení škodlivého XUL kódu do zdrojového kódu stránky získa možnosť vykonania ďalšieho škodlivého kódu.

Zraniteľnosť CVE-2017-7800 spočíva v opätovnom využití uvoľnenej pamäte v komponente WebSockets, keď objekt zodpovedajúci za spojenie je uvoľnený ešte pred dokončením operácie odpájania. Zneužitie tejto zraniteľnosti spôsobí potenciálne zneužiteľné zrútenie sa aplikácie.

Zraniteľnosť CVE-2017-7801 spočíva v opätovnom využití uvoľnenej pamäte pri prepočítavaní rozloženia stránky pre „marquee“ element počas zmien veľkosti okna, pričom aktualizovaný objekt je uvoľnený z pamäte zatiaľ čo sa stále používa. Toto môže spôsobiť zneužiteľné zrútenie sa aplikácie.

Zraniteľnosti CVE-2017-7779 a CVE-2017-7780 obsahujú viacero chýb v správe pamäte a predpokladá sa, že je možné ich zneužiť pre vykonanie ľubovoľného kódu.

Zraniteľné systémy:
Mozilla Firefox ESR 52.2.1 a staršie
Mozilla Firefox 54.0.1 a staršie

Odporúčania:
Odporúčame aktualizovať prehliadač Mozilla Firefox na verzie 55.0.3 (opravy uvedených zraniteľností sú zahrnuté už vo verzii 55.0) a ESR 52.3. Prehliadač Firefox ponúka aktualizácie automaticky po ich zverejnení. Ak sa tak nestalo, aktualizáciu je možné spustiť manuálne otvorením Menu > Pomocník > O prehliadači Firefox. Kontrola aktualizácie sa spustí súčasne so zobrazením okna s informáciami o aktuálnej verzii.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/mfsa2017-19/
https://www.mozilla.org/en-US/security/advisories/mfsa2017-18/#CVE-2017-7798

Google Chrome

Spoločnosť Google v auguste vydala tri aktualizácie pre prehliadač Chrome, avšak v rámci žiadnej z nich neboli zverejnené informácie o prípadných opravách zraniteľností.

Zraniteľné systémy:
Google Chrome 60.0.3112.113 a staršie

Odporúčania:
Odporúčame overiť, či sa prehliadač Chrome automaticky aktualizoval na najnovšiu verziu 61.0.3163.79, 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/2017/07/stable-channel-update-for-desktop.html

4. Adobe

Adobe Flash Player

Spoločnosť Adobe vydala v mesiaci august opravy dvoch zraniteľností v aplikáciách Adobe Flash Player. Kritická zraniteľnosť CVE-2017-3106 umožňuje vykonanie škodlivého kódu na diaľku, a to zneužitím nesprávnej konverzie typu objektu, zdroja alebo štruktúry pri spracovaní SWF súborov. Pre túto zraniteľnosť existuje verejne dostupný exploit.

Zraniteľnosť CVE-2017-3085, označená ako dôležitá, spočíva v narábaní s externými zdrojmi a umožňuje útočníkovi pristúpiť k citlivým informáciám aktuálne prihláseného používateľa. K úspešnému zneužitiu je potrebné, aby užívateľ navštívil webovú stránku so škodlivým obsahom alebo otvoril súbor so škodlivým kódom.

Zraniteľné systémy:
Adobe Flash Player Desktop Runtime 26.0.0.131 a staršie (Windows, Macintosh a Linux)
Adobe Flash Player pre Google Chrome 26.0.0.131 a staršie (Windows, Macintosh, Linux a Chrome OS)
Adobe Flash Player pre Microsoft Edge a Internet Explorer 11 26.0.0.131 a staršie (Windows 10 a 8.1)

Odporúčania:
Odporúčame aktualizovať Flash Player na verziu 26.0.0.151. 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/apsb17-23.html
http://www.zerodayinitiative.com/advisories/ZDI-17-634/
https://get.adobe.com/flashplayer/

5. Frameworky

Microsoft .NET

Spoločnosť Microsoft v auguste nevydala žiadne opravy zraniteľností pre .NET.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/b3d96835-f651-e711-80dd-000d3a32fc99

Oracle Java SE

Spoločnosť Oracle v auguste nevydala žiadne opravy zraniteľností. Najbližší balík opráv má byť vydaný 17. októbra 2017.

Zdroje:
http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html

6. Iné závažné zraniteľnosti

Zero-day zraniteľnosti v softvéri Foxit Reader

Koncom augusta boli spoločnosťou Foxit vydané opravy dvoch zero-day zraniteľností v softvéri Foxit Reader. Prvá z nich, CVE-2017-10951, spočívajúca v nesprávnom spracovaní používateľského vstupu, umožňuje útočníkovi vykonať príkaz na napadnutom zariadení, a tým ďalej na diaľku vykonať škodlivý kód v kontexte procesu Foxit Reader. Pre úspešné zneužitie zraniteľnosti je potrebné, aby používateľ navštívil pripravenú škodlivú stránku alebo otvoril súbor so škodlivým obsahom.

Druhou opravenou zero-day zraniteľnosťou je CVE-2017-10952, ktorá spočíva v nedostatočnom overení používateľských vstupných dát. Zraniteľnosť umožňuje útočníkovi vykonať na diaľku škodlivý kód v kontexte aktuálneho procesu. Pre úspešné zneužitie zraniteľnosti je potrebné, aby používateľ navštívil pripravenú škodlivú stránku alebo otvoril súbor so škodlivým obsahom.

Zraniteľné systémy:
Foxit Reader 8.3.1 a staršie

Odporúčania:
Odporúčame čo najskôr aktualizovať Foxit Reader na opravenú verziu 8.3.2.

Zdroje:
https://www.foxitsoftware.com/pdf-reader/version-history.php

Zraniteľnosti v Cisco Application Policy Infrasctructure Controller

V auguste vydala spoločnosť Cisco opravu kritickej zraniteľnosti CVE-2017-6767 v Cisco Application Policy Infrasctructure Controller (APIC - Centrálny riadiaci element Cisco ACI sietí). Zraniteľnosť spočíva v chybe pri prideľovaní právomocí pri prihlásení k ovládaciemu rozhraniu APIC cez SSH. Autentifikovaný vzdialený útočník by mohol zneužiť túto zraniteľnosť na povýšenie svojich právomocí na úroveň posledného používateľa, prihláseného cez SSH a následne vykonávať cez terminál príkazy. V tomto prípade vzdialený útočník nemá možnosť získať root právomoci.

Druhou opravenou kritickou zraniteľnosťou v Cisco APIC je kritická zraniteľnosť CVE-2017-6768 spočívajúca v chybe pri overení načítavanej knižnice pri použití relatívnych ciest. Lokálny autentifikovaný útočník môže túto zraniteľnosť zneužiť na povýšenie svojich právomocí až na úroveň root prostredníctvom načítania škodlivej knižnice.

Zraniteľné systémy:

Cisco APIC staršie ako 2.0
Cisco APIC 2.0
Cisco APIC 2.1
Cisco APIC 2.2
Cisco APIC 2.3

Odporúčania:

V prípade všetkých verzií starších ako 2.3 odporúčame migrovať systém na verziu 2.2(2e). V prípade používania verzie 2.2 odporúčame aktualizovať rovnako na verziu 2.2(2e). Nakoniec, v prípade používania verzie APIC 2.3, odporúčame aktualizovať na verziu 2.3(1f).

Zdroje:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-apic1
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-apic2