Mesačný prehľad kritických zraniteľností

November 2017

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft v rámci novembrového balíka aktualizácií nevydala vydala opravu žiadnej kritickej zraniteľnosti.

Pre dôležitú zraniteľnosť CVE-2017-11830, však existuje verejne dostupný exploit. Ide o obídenie bezpečnostného prvku, keď komponent Device Guard vo Windows Defender-i, nesprávne vyhodnotí nedôveryhodný súbor. Úspešným zneužitím môže útočník spôsobiť, že nepodpísaný súbor sa bude javiť ako podpísaný. Keďže Device Guard sa pri rozlišovaní škodlivých súborov spolieha na podpisy, môže následne povoliť vykonanie škodlivého súboru.

Zraniteľné systémy:

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 10 Version 1709 for 32-bit Systems
Windows 10 Version 1709 for x64-based Systems
Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows Server, version 1709 (Server Core Installation)

Odporúčania:

Vzhľadom na výskyt verejne dostupného exploitu 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-2017-11830

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft v rámci novembrového balíka aktualizácií nevydala vydala opravu žiadnej kritickej zraniteľnosti. Avšak k jednej z dôležitých zraniteľností, CVE-2017-11882, existuje verejne dostupný exploit.

Uvedená zraniteľnosť umožňuje útočníkovi na diaľku vykonať škodlivý kód. Táto zraniteľnosť spočíva v narušení integrity pamäte, keď v softvéri zlyhá spáva objektov v pamäti. Úspešné zneužitie umožní útočníkovi na diaľku vykonať škodlivý kód s právomocami práve prihláseného používateľa. Ak je užívateľ prihlásený ako správca, môže to znamenať prevzatie kontroly nad napadnutým systémom. 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 2007 Service Pack 3
Microsoft Office 2010 Service Pack 2 (32-bit and 64-bit editions)
Microsoft Office 2013 Service Pack 1 (32-bit and 64-bit editions)
Microsoft Office 2016 (32-bit and 64-bit editions)

Odporúčania:
Vzhľadom na výskyt verejne dostupného exploitu 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-2017-11882
https://threatpost.com/microsoft-patches-20-critical-vulnerabilities/128891/

3. Internetové prehliadače

Microsoft Internet Explorer

V rámci novembrového balíka opráv boli spoločnosťou Microsoft vydané opravy kritických zraniteľností CVE-2017-11837, CVE-2017-11838, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858 a CVE-2017-11869 v skriptovacom engine, ktoré útočníkovi umožňujú spôsobiť narušenie integrity pamäte a následne vzdialene vykonať škodlivý kód v kontexte práve prihláseného používateľa. Pre úspešné zneužitie potrebuje útočník pripraviť špeciálnu webovú stránku, alebo škodlivý webový obsah a nalákať používateľa na navštívenie danej stránky. Inou možnosťou je umiestnenie škodlivého obsahu do Microsoft Office dokumentu, otvorením ktorého rovnako dôjde ku zneužitiu zraniteľností.

Kritické zraniteľnosti CVE-2017-11855 a CVE-2017-11856 v prehliadači Internet Explorer 11 spočívajú 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, prípadne stránku so zdieľaným používateľským obsahom, a následne nalákať používateľa na navštívenie danej stránky.

Zraniteľné systémy:
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-2017-11837
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11838
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11843
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11846
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11858
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11869
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11855
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11856

Microsoft Edge

V rámci novembrového balíka aktualizácií boli pre prehliadač Microsoft Edge vydané opravy kritických zraniteľností CVE-2017-11837, CVE-2017-11838, CVE-2017-11843, CVE-2017-11846 a CVE-2017-11858, ktoré sú spoločné s prehliadačom Internet Explorer 11 a ktorých popis je uvedený v predošlej časti.

Kritické zraniteľnosti CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11861, CVE-2017-11870 a CVE-2017-11873 v skriptovacom engine Chakra spočívajú v chybnom narábaní s objektami 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. Na všetky vyššie uvedené zraniteľnosti sú verejne dostupné exploity.

Ďalšie novembrové aktualizácie sa týkajú kritických zraniteľností CVE-2017-11836, CVE-2017-11845, CVE-2017-11862, CVE-2017-11866 a CVE-2017-11871 v skriptovacom engine, ktoré rovnako ako aj tie predošlé spočívajú v chybnom narábaní s objektami v pamäti. Útočník môže spôsobiť narušenie integrity pamäte a tak získať 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.

Zraniteľné systémy:

Microsoft Edge v systémoch Windows 10 verzií 1511, 1607 a 1703 v 32-bitových aj 64-bitových verziách
Microsoft Edge v systéme Windows Server 2016

Odporúčania:

Vzhľadom na verejnú dostupnosť 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-2017-11839
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11861
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11870
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11873
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11836
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11845
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11862
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11866
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11871

Mozilla Firefox

Spoločnosť Mozilla v novembri vydala opravy piatich kritických zraniteľností v prehliadačoch Firefox.

Aktualizovaná verzia Firefox 57.0 obsahuje 15 opravených zraniteľností, z ktorých 3 boli kritické.

Kritická zraniteľnosť CVE-2017-7828 spočíva v umožnení opätovného využitia uvoľnenej pamäte. K chybe môže dôjsť počas zmien v layoute, keď sa uvoľní objekt v komponente PressShell, hoci sa stále používa. Dôsledkom môže byt potenciálne zneužiteľne zrútenie sa aplikácie.

Zraniteľnosti pod označeniami CVE-2017-7826 a CVE-2017-7827 spočívajú v narušení integrity pamäte. Úspešným zneužitím môže útočník vykonať škodlivý kód na napadnutom systéme.

Aktualizovaná verzia Firefox ESR 52.5.0 obsahuje 3 opravené zraniteľnosti, z ktorých 2 boli kritické. Ide o tie isté zraniteľnosti, CVE-2017-7828 a CVE-2017-7826, ako v prehliadačoch Firefox 57.0.

Pre úspešné zneužitie spomenutých kritických zraniteľností musí byť užívateľ nalákaný na navštívenie špeciálnej stránky so škodlivým obsahom.

Zraniteľné systémy:

Mozilla Firefox 57.0 a staršie
Mozilla Firefor ESR 52.4.1 a staršie

Odporúčania:

Hoci na stránkach spoločnosti ešte nie sú uverejnené detaily o verzii 57.0.1 vydanej 29. novembra, odporúčame aktualizovať prehliadač Mozilla Firefox na najnovšie verzie 57.0.1 a ESR 52.5.0. 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/
https://www.mozilla.org/en-US/security/advisories/mfsa2017-24/
https://www.mozilla.org/en-US/security/advisories/mfsa2017-25/
https://access.redhat.com/security/cve/cve-2017-7828
https://access.redhat.com/security/cve/cve-2017-7826

Google Chrome

Spoločnosť Google v novembri vydala dve aktualizácie pre prehliadač Chrome.

V rámci prvej aktualizácie zo 6.11., verzia Google Chrome 62.0.3202.89, boli opravené dokopy 2 zraniteľnosti, z toho 1 kritická. Kritická zraniteľnosť CVE-2017-15398 je v protokole QUIC a umožňuje spôsobiť pretečenie zásobníka.

V rámci aktualizácie z 13.11. bola opravená 1 kritická zraniteľnosť, CVE-2017-15428. Príčina zraniteľnosti je vo V8 JavaScript engine, ktorý umožňuje zápis mimo pridelenú pamäť.

Zraniteľné systémy:
Google Chrome 62.0.3202.89 a staršie

Odporúčania:
Odporúčame overiť, či sa prehliadač Chrome automaticky aktualizoval na najnovšiu verziu 62.0.3202.94. 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/2017/11/stable-channel-update-for-desktop_13.html
https://chromereleases.googleblog.com/2017/11/stable-channel-update-for-desktop.html

4. Adobe

Adobe Flash Player

Spoločnosť Adobe vydala v novembri opravy piatich kritických zraniteľností v aplikácii Adobe Flash Player.

Každá zo zraniteľností môže viesť k vzdialenému vykonaniu škodlivého kódu. K úspešnému útoku je vo všetkých prípadoch nutná interakcia používateľa, napr. otvorenie špeciálne pripraveného súbor používateľom, ktorý môže byť umiestnený napríklad na webovej stránke alebo v prílohe emailu.

Úspešné zneužitie zraniteľností CVE-2017-3112, CVE-2017-3114 a CVE-2017-11213 umožní útočníkovi čítanie mimo pridelenej pamäte.

Zraniteľnosti CVE-2017-11215 a CVE-2017-11225 spočívajú v umožnení opätovného využitia predtým uvoľnenej pamäte.

Zraniteľné systémy:
Adobe Flash Player Desktop Runtime 27.0.0.183 a staršie (Windows, Macintosh a Linux)
Adobe Flash Player for Google Chrome 27.0.0.183 a staršie (Windows, Macintosh, Linux a Chrome OS)
Adobe Flash Player for Microsoft Edge and Internet Explorer 11 27.0.0.183 a staršie (Windows 10 a 8.1)

Odporúčania:
Odporúčame aktualizovať Adobe Flash Player na najnovšiu verziu 27.0.0.187. 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/apsb17-33.html
https://threatpost.com/adobe-patches-flash-player-56-bugs-in-reader-and-acrobat/128876/
https://access.redhat.com/security/cve/cve-2017-3112
https://access.redhat.com/security/cve/cve-2017-3114
https://access.redhat.com/security/cve/cve-2017-11213
https://access.redhat.com/security/cve/cve-2017-11215
https://access.redhat.com/security/cve/cve-2017-11225
https://get.adobe.com/flashplayer/

5. Frameworky

Microsoft .NET

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

Z dôležitých zraniteľností 2 umožňujú spôsobenie obmedzenie dostupnosti služby (DoS). Zraniteľnosť CVE-2017-11770 existuje v komponente .NET Core a spočíva v nesprávnom spravovaní certifikátov. Vzdialený útočník bez overenia môže zneužiť túto zraniteľnosť poskytnutím špeciálne pripraveného certifikátu aplikácii .NET Core. Zraniteľnosť CVE-2017-11883 je spôsobená nesprávnym spracovaním webových žiadostí aplikáciou ASP.NET Core. Vzdialený útočník bez overenia môže zneužiť túto zraniteľnosť zaslaním špeciálne pripravenej žiadosti aplikácii .NET Core.

Dôležitá zraniteľnosť, CVE-2017-11879, umožňuje povýšenie právomocí. Spočíva v umožnení presmerovania na inú stránku pri spracovaní parametrov „http get“ žiadosti. Pre zneužitie zraniteľnosti je potrebné presvedčiť používateľa kliknúť na špeciálny odkaz. Keď autentifikovaný používateľ klikne na takýto link, relácia prehliadača môže byť presmerovaná na škodlivý stránku navrhnutú k získaniu informácií ako sú cookies alebo autentifikačné tokeny.

Ďalšia dôležitá zraniteľnosť, CVE-2017-8700, umožňuje sprístupnenie dôverných informácií a to obídením CORS (Cross-origin Resource Sharing) konfigurácií ASP.NET Core. Úspešné zneužitie zraniteľnosti môže viesť k získaniu obsahu, ku ktorému webové aplikácie bežne nemajú prístup.

Zraniteľné systémy:
Microsoft .NET 1.0
Microsoft .NET 1.1
Microsoft .NET 2.0
Microsoft ASP.NET Core 1.0
Microsoft ASP.NET Core 1.1
Microsoft ASP.NET Core 2.0

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-2017-11770
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11883
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11879
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8700

Oracle Java SE

Spoločnosť Oracle v mesiaci september nevydala žiadne opravy zraniteľností. Najbližší balík opráv má byť vydaný 16. januára 2017.

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

6. Iné závažné zraniteľnosti

Kritická zraniteľnosť v procesoroch od spoločnosti Intel

Koncom novembra bola zverejnená informácia o kritických zraniteľnostiach vo firmvéroch Intel Management Engine (ME), Intel Trusted Execution Engine (TXE) a Intel Server Platform Services (SPS). Všetky funkcie ME, SPS alebo TXE sú štandardne zapnuté. Zneužitím týchto zraniteľností môže útočník vykonať škodlivý kód, a to mimo viditeľnosti používateľa a operačného systému, alebo spôsobiť zrútenie systému a obísť všetky štandardné bezpečnostné prvky. Prvé tri zraniteľnosti (CVE-2017-5705, CVE-2017-5706 a CVE-2017-5707) boli identifikované v októbri výskumníkmi z Positive Technologies a následne bolo spoločnosťou Intel identifikovaných ďalších 5 zraniteľností.

Zraniteľnosti CVE-2017-5705, CVE-2017-5711, CVE-2017-5712*, CVE-2017-5706, CVE-2017-5707 spočívajú v pretečení zásobníkov v spomenutých firmvéroch (ME, TXE a SP) a umožňujú útočníkovi s lokálnym prístupom vykonať škodlivý kód.

Zraniteľnosti CVE-2017-5708, CVE-2017-5709 a CVE-2017-5710 umožňujú povýšenie právomocí útočníkovi s lokálnym prístupom.

K zneužitiu všetkých uvedených zraniteľností potrebuje mať útočník lokálny alebo fyzický prístup k systémom.

* Túto zraniteľnosť je možne zneužiť aj cez vzdialený prístup, ale len s platným administrátorským overením do Intel ME.

Zraniteľné systémy:

Intel ME Firmware verzie 11.0.0 až 11.7.0
SPS Firmware verzia 4.0
TXE verzia 3.0

Uvedené verzie firmvérov sa vyskytujú napríklad v procesoroch:

6th, 7th & 8th Generation Intel Core Processor Family
Intel Xeon Processor E3-1200 v5 & v6 Product Family
Intel Xeon Processor Scalable Family
Intel Xeon Processor W Family
Intel Atom C3000 Processor Family
Apollo Lake Intel Atom Processor E3900 series
Apollo Lake Intel Pentium
Celeron G, N and J series Processors

Odporúčania:

Odporúčame navštíviť stránku spoločnosti Intel – prvý odkaz v sekcii zdroje, kde sú informácie o možnostiach aktualizácie firmvéru, prípadne odkazy na výrobcov.

Zdroje:

https://www.intel.com/content/www/us/en/support/articles/000025619/software.html
https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00086&languageid=en-fr
https://threatpost.com/intel-patches-cpu-bugs-impacting-millions-of-pcs-servers/128962/

Kritická zero-day zraniteľnosť v mailovom systéme Exim

Koncom novembra boli zverejnené informácie o kritických zero-day zraniteľnostiach v mailovom systéme Exim, o čom aj CSIRT.SK informoval vo varovaní na svojej stránke. Zraniteľnosti CVE-2017-16943 a CVE-2017-16944 spočívajú v chybnom spracovaní prijatých správ, kedy vzdialený útočník môže pomocou BDAT príkazov získať možnosť vzdialeného vykonania kódu, prípadne spôsobiť zrútenie aplikácie. Kód demonštrujúci existenciu zraniteľnosti je už verejne dostupný a je otázkou času, kedy bude útočníkmi pretvorený na reálny exploit.

Zraniteľné systémy:

Exim 4.88
Exim 4.89

Odporúčania:

Oprava uvedených zraniteľností zatiaľ nebola vydaná. Na zmiernenie rizika odporúčame vypnúť podporu oznamovania rozšírenia ESMTP CHUNKING. V konfigurácii Eximu je potrebné uviesť riadok "chunking_advertise_hosts=". Správcom systémov odporúčame pravidelne kontrolovať dostupnosť aktualizácií a čo najskôr aktualizovať na opravenú verziu.

Zdroje:

https://lists.exim.org/lurker/message/20171125.034842.d1d75cac.en.html
https://nvd.nist.gov/vuln/detail/CVE-2017-16943
https://nvd.nist.gov/vuln/detail/CVE-2017-16944