Mesačný prehľad kritických zraniteľností

December 2017

1. Operačné systémy Microsoft Windows

V mesiaci december vydala spoločnosť Microsoft opravy 2 kritických zraniteľností v operačných systémoch Windows. Kritické zraniteľnosti CVE-2017-11937 a CVE-2017-11940 umožňujú útočníkovi na diaľku vykonať škodlivý kód s právomocami LocalSystem. K tomu je potrebný špeciálne navrhnutý súbor, ktorý pri skenovaní pomocou Microsoft Malware Protection Engine spôsobí narušenie integrity pamäte. Takýto súbor môže útočník šíriť napríklad pomocou webstránky, e-mailom, alebo správou cez Instant Messenger. Zneužiť túto zraniteľnosť je možné aj na serveroch, ktoré obsahujú stránky s užívateľským obsahom. Nahraný súbor do zdieľanej oblasti môže byť skenovaný Microsoft Malware Protection Engine bežiacom na danom serveri, čím dôjde ku zneužitiu zraniteľnosti. Úspešným zneužitím môže útočník prevziať kontrolu nad napadnutým systémom, inštalovať programy, prehliadať, meniť a zmazať dáta, a vytvárať nové užívateľské kontá.

Zraniteľné súčasti:

Microsoft Exchange Server 2013

Microsoft Exchange Server 2016

Microsoft Forefront Endpoint Protection 2010

Microsoft Security Essentials

Windows Defender

Windows Intune Endpoint Protection

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 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 64-based Systems

Windows RT 8.1

Windows Server 2016

Windows Server 2016 (Server Core Installation)

Windows Server, version 1709 (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-2017-11937
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11940

2. Kancelárske balíky Microsoft Office a Office Web Apps

V mesiaci december nevydala spoločnosť Microsoft žiadne opravy kritických zraniteľností pre Microsoft Office.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance

3. Internetové prehliadače

Microsoft Internet Explorer

V rámci decembrového balíka opráv boli spoločnosťou Microsoft vydané opravy kritických zraniteľností CVE-2017-11886, CVE-2017-11891, CVE-2017-11890, CVE-2017-11903 a CVE-2017-11907 v skriptovacom engine prehliadača, spočívajúce v chybách pri prístupe ku objektom v pamäti. Útočník má možnosť 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. Exploity na posledné tri menované zraniteľnosti sú verejne dostupné.

V decembri boli vydané opravy kritických zraniteľností CVE-2017-11894, CVE-2017-11895, CVE-2017-11912 a CVE-2017-11930 spočívajúcich 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, prípadne stránku so zdieľaným používateľským obsahom, a následne nalákať používateľa na navštívenie danej stránky. Druhou možnosťou je umiestnenie JavaScript obsahu do Microsoft Office dokumentu, otvorením ktorého rovnako dôjde ku zneužitiu zraniteľností.

Spoločnosť Microsoft tiež vydala opravu zraniteľnosti CVE-2017-11906, označenej ako dôležitá. Zraniteľnosť spočíva v chybe v narábaní s objektami v pamäti a umožňuje útočíkovi spôsobiť únik informácií, ktoré možno potenciálne zneužiť na ďalšie pokračovanie v útoku. Pre úspešné zneužitie útočník potrebuje vytvoriť webovú stránku so škodlivým obsahom, prípadne tento obsah umiestniť na stránky so zdieľaným používateľským obsahom a následne nalákať používateľa na navštívenie danej stránky. Exploit na túto zraniteľnosť je verejne dostupný.

Zraniteľné systémy:
Microsoft Internet Explorer 11

Odporúčania:
Vzhľadom na existenciu 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-2017-11907
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11930

Microsoft Edge

V rámci decembrového balíka aktualizácií boli vydané opravy kritických zraniteľností CVE-2017-11889, CVE-2017-11893, CVE-2017-11905, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11914 a CVE-2017-11918 v skriptovacom engine prehliadača, ktoré spočívajú v chybe pri 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.

V decembri bola vydaná oprava kritickej zraniteľnosti CVE-2017-11888 v prehliadači Edge, ktorá spočíva v chybnom prístupe ku 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.

Spoločnosť Microsoft v decembri vydala pre prehliadač Edge opravu kritických zraniteľností CVE-2017-11894, CVE-2017-11895 a CVE-2017-11912 v skriptovacom engine, ktoré umožňuju 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 Microsoft Office dokumentu, otvorením ktorého rovnako dôjde ku zneužitiu zraniteľnosti.

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:

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-2017-11918
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11888
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11912

Mozilla Firefox

Spoločnosť Mozilla vydala v decembri opravu jednej kritickej zraniteľnosti v prehliadači Firefox. Táto zraniteľnost, CVE-2017-7845, sa týka pretečenia medzipamäte pri vykresľovaní a overovaní prvkov pomocou knižnice ANGLE s použitím Direct 3D 9 (WebGL obsah). Predpokladá sa, že spôsobený pád programu je zneužiteľný.

Zraniteľné systémy:

Mozilla Firefox 57.0.1 a staršie

Mozilla Firefox ESR 52.5.1 a staršie

Odporúčania:

Odporúčame aktualizovať prehliadač Mozilla Firefox na verzie 57.0.2, resp. ESR 52.5.2. Prehliadač Firefox aj 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/mfsa2017-29/
https://www.mozilla.org/en-US/security/advisories/mfsa2017-28/

Google Chrome

Spoločnosť Google v decembri vydala dve aktualizácie pre prehliadač Chrome, v rámci ktorých bolo opravených celkovo 39 zraniteľností. Kritická zraniteľnosť CVE-2017-15407 v QUIC (sieťový protokol) spočívajúca v zápise pamäte mimo pridelený rozsah mohla útočníkovi pravdepodobne umožniť vzdialené vykonanie škodlivého kódu.

V komponente PDFium boli vydané opravy pre zraniteľnosti CVE-2017-15410, CVE-2017-15411 a CVE-2017-15408, označené ako dôležité, ktoré spočívajú v chybách pri správe pamäte. Zraniteľnosti rovnakého typu a závažnosti CVE-2017-15409 a CVE-2017-15412 boli opravené v komponentoch Skia (grafická knižnica) a libXML.

V decembri bola tiež vydaná oprava pre zraniteľnosť CVE-2017-15429 v JavaScript engine V8, označenú ako dôležitá. Zraniteľnosť spočíva v možnosto pre útočníka vykonať útok typu UXSS (universal cross-site scripting).

Zraniteľné systémy:
Google Chrome 63.0.3239.84 a staršie

Odporúčania:
Odporúčame overiť, či sa prehliadač Chrome automaticky aktualizoval na najnovšiu verziu 63.0.3239.132, 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/
https://chromereleases.googleblog.com/2017/12/stable-channel-update-for-desktop_14.html
https://chromereleases.googleblog.com/2017/12/stable-channel-update-for-desktop.html

4. Adobe

Adobe Flash Player

Spoločnosť Adobe vydala v decembri opravu jednej kritickej zraniteľnosti v aplikácii Adobe Flash Player. Ide o zraniteľnosť CVE-2017-11305, ktorá môže spôsobiť nechcený reset súboru s globálnymi nastaveniami.

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:
Odporúčame aktualizovať Adobe Flash Player na verziu 28.0.0.126. 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/apsb17-42.html
https://get.adobe.com/flashplayer/

5. Frameworky

Microsoft .NET

V rámci decembrového balíka aktualizácií spoločnosť Microsoft nevydala žiadne opravy zraniteľností vo frameworku.NET.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance

Oracle Java SE

Spoločnosť Oracle v mesiaci december nevydala žiadne opravy zraniteľností. Najbližší balík opráv má byť vydaný 16. januára 2018.

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

6. Iné závažné zraniteľnosti

Kritická zraniteľnosť v mailovom klientovi Mozilla Thunderbird

Spoločnosť Mozilla vydala v decembri opravu kritickej zraniteľnosti CVE-2017-7845 v poštovom klientovi Thunderbird (rovnaká ako v prehliadači Firefox), ktorá spočíva v pretečení medzipamäte pri vykresľovaní a overovaní prvkov pomocou knižnice ANGLE s použitím Direct 3D 9 (WebGL obsah). Predpokladá sa, že spôsobený pád programu je zneužiteľný.

Zraniteľné systémy:
Mozilla Thunderbird 52.5.1 a staršie

Odporúčania:
Odporúčame aktualizovať prehliadač poštový klient Thunderbird na verziu 52.5.2. Klient Thunderbird ponúka aktualizácie automaticky po ich zverejnení. Ak sa tak nestalo, aktualizáciu je možné spustiť manuálne otvorením Menu > Pomocník > O klientovi Thunderbird. Kontrola aktualizácie sa spustí súčasne so zobrazením okna s informáciami o aktuálnej verzii.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/mfsa2017-30/

Kritická zraniteľnosť v správcovi hesiel Keeper

V decembri boli zverejnené informácie o kritickej zraniteľnosti v správcovi hesiel Keeper. Tento softvér zvykne byť predinštalovaný na operačných systémoch Windows 10. Zraniteľnosť sa týka komponentu Keeper Browser Extension. Vzdialený útočník môže pripraviť škodlivú stránku a nalákať používateľa na jej navštívenie. Fingovaním používateľského vstupu môže spôsobiť vykonanie privilegovaného kódu v Keeper Browser Extension, čo spôsobí odoslanie hesiel útočníkovi, pokiaľ je používateľ práve prihlásený do aplikácie Keeper.

Zraniteľné systémy:
Keeper Browser Extension 11.3

Odporúčania:
Odporúčame preveriť, či sa doplnok Keeper Browser Extension vo vašich prehliadačoch aktualizoval na verziu 11.4.4, prípadne novšiu. V prípade potreby je možné najnovšiu verziu stiahnuť na druhom odkaze nižšie.

Zdroje:
https://blog.keepersecurity.com/2017/12/15/update-for-keeper-browser-extension-v11-4/
https://keepersecurity.com/download.html