Mesačný prehľad kritických zraniteľností

Apríl 2017

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft v apríli vydala aktualizácie na opravu viacerých zraniteľností:
Zraniteľnosť CVE-2017-0158 vo VBScript engine umožňuje útočníkovi zneužiť chybu v správe objektov v pamäti a pomocou špeciálne vytvorenej webstránky vykonať škodlivý kód, pričom je potrebná interakcia používateľa.

Kritické zraniteľnosti CVE-2017-0162, CVE-2017-0163, CVE-2017-0180 a CVE-2017-0181 v komponente Hyper-V Network Switch umožňujú útočníkovi využiť chybu pri spracovaní vstupu od používateľa. Spustením špeciálne pripraveného kódu na hosťovskom systéme dokáže útočník spôsobiť vykonanie škodlivého kódu na hostiteľskom systéme.

Spoločnosť Microsoft od apríla končí s vydávaním Microsoft Security Bulletinov, ktoré budú nahradené Security Updates Guide.

Spoločnosť Microsoft v apríli oznámila koniec podpory operačného systému Windows Vista a tiež viacerých ďalších produktov (viď spodnú tabuľku).

Zraniteľné systémy:
Windows Vista Service Pack 2
Windows Vista x64 Edition Service Pack 2
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

Ukončenie podpory:
Windows Vista SP2
Microsoft BizTalk Adapters for Host Systems
Microsoft BizTalk FileAct and InterAct Adapters for SWIFT
Microsoft Dynamics NAV 5.0
Microsoft Exchange Server 2007
Microsoft Expression Web
Microsoft Host Integration Server 2006
Microsoft Office Communicator Phone Edition
Microsoft Office InterConnect 2007
Microsoft Visual Studio 2005 Team Edition for Database Professionals
Internet Explorer 9 vo Windows Vista SP2

Odporúčania:
Aplikovať aktualizácie, publikované prostredníctvom služby Windows Update, pre príslušný operačný systém. Číslo aktualizácie pre konkrétny systém možno vyhľadať na nižšie uvedenej stránke vložením kódu chyby do vyhľadávania.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0158
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0162
https://support.microsoft.com/en-us/help/4001737/products-reaching-end-of-support-for-2017
https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet

2. Kancelárske balíky Microsoft Office a Office Web Apps

V rámci aprílového balíka aktualizácií spoločnosť Microsoft vydala kritickú opravu zero-day zraniteľnosti CVE-2017-0199, ktorá útočníkovi prostredníctvom špeciálne vytvoreného súboru umožňovala vzdialené vykonanie škodlivého kódu a kontrolu nad napadnutým systémom. Táto zraniteľnosť sa okrem Microsoft Office týka aj programu WordPad.

Tiež bola vydaná oprava kritickej zraniteľnosti CVE-2017-0106 v programe Outlook, ktorá útočníkovi pomocou špeciálne vytvorenej emailovej správy umožňuje získať kontrolu nad napadnutým systémom a spúšťať škodlivý kód.

Zraniteľné systémy:
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 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition).

WordPad:
Windows Vista Service Pack 2
Windows Vista x64 Edition Service Pack 2
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1

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

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 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)

Odporúčania:
Aplikovať balíky aktualizácií, publikované prostredníctvom služby Windows Update, nakoľko výskyt exploitov je v blízkej budúcnosti pravdepodobný. Čísla aktualizácií pre konkrétnu verziu Microsoft Office a danú zraniteľnosť možno vyhľadať na prvých troch uvedených odkazoch.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0106
https://www.exploit-db.com/exploits/41894/

3. Internetové prehliadače

Microsoft Internet Explorer

Vydané aktualizácie ošetrujú dve kritické zraniteľnosti, ktoré umožňujú vzdialené vykonanie škodlivého kódu prostredníctvom navštívenia webovej stránky s pripraveným škodlivým obsahom, vzhľadom na čo je potrebná interakcia používateľa. Zraniteľnosť CVE-2017-0201 umožňuje útočníkovi narušiť integritu pamäte zneužitím chyby v narábaní s pamäťou v JScript a VBScript komponentoch. Podobne zraniteľnosť CVE-2017-0202 umožňuje spôsobiť porušenie integrity pamäti zneužitím chyby v prístupe IE ku niektorým objektom v pamäti.

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

Odporúčania:
Odporúčame používateľom a správcom čo najskôr aplikovať aktualizácie cez službu Windows Update, nakoľko na druhú menovanú zraniteľnosť je exploit verejne dostupný. Číslo aktualizácie pre konkrétnu verziu možno vyhľadať navštívením prvého z nižšie uvedených odkazov a vložením kódu chyby do vyhľadávania.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0201

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0202
https://www.exploit-db.com/exploits/41941/

Microsoft Edge

Aprílový balík aktualizácií pre Microsoft Edge ošetruje tri kritické zraniteľnosti CVE-2017-0093, CVE-2017-0200 a CVE-2017-205, umožňujúce spôsobiť narušenie integrity pamäti zneužitím chýb v narábaní s pamäťou. Útočník môže presvedčiť používateľa navštíviť pripravenú stránku so škodlivým obsahom a následne vzdialene vykonať škodlivý kód.

Zraniteľné systémy:
Microsoft Edge na systémoch Windows 10 verzií 1511, 1607 a 1730 v 32-bit aj x64 prevedení.

Odporúčania:
Vzhľadom na vysokú pravdepodobnosť výskytu exploitov na uvedené zraniteľnosti odporúčame používateľom a správcom aplikovať balíky aktualizácií, publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétnu verziu možno vyhľadať navštívením uvedeného odkazu a nastavením filtra pre Microsoft Edge.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0093
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0200
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0205

Mozilla Firefox

Spoločnosť Mozilla vydala v mesiaci apríl balíky aktualizácií na opravu viacerých kritických zraniteľností v správe pamäti, ako použitie uvoľnenej pamäte (CVE-2017-5433, CVE-2017-5435), zápis mimo pridelenej pamäte (CVE-2017-5436, CVE-2017-5461) a pretečenie zásobníka (CVE-2017-5459). Úspešné zneužitie týchto zraniteľností spôsobuje zrútenie aplikácie, ktoré je možné potenciálne zneužiť ďalej. Kritické zraniteľnosti CVE-2017-5430 a CVE-2017-5429 umožňujú útočníkovi využiť chyby v narábaní s pamäťou za účelom vzdialeného vykonania škodlivého kódu. Zraniteľnosť CVE-2017-5466 umožňuje útočníkovi uskutočniť XSS útok po tom, ako používateľ navštívi stránku so škodlivým obsahom, čo môže viesť k úniku dát.

Zraniteľné systémy:
Mozilla Firefox 45.9 ESR
Mozilla Firefox 52.1 ESR
Mozilla Firefox 53

Odporúčania:
Odporúčame aktualizovať Firefox na najnovšiu verziu. 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/mfsa2017-10/
https://www.mozilla.org/en-US/security/advisories/mfsa2017-11/
https://www.mozilla.org/en-US/security/advisories/mfsa2017-12/

Google Chrome

Spoločnosť Google vydala v apríli aktualizácie ošetrujúce kritické zraniteľnosti v správe pamäti a v komponentoch PDFium a Blink. Ich zneužitie vo všetkých prípadoch umožňuje vzdialené vykonanie škodlivého kódu.

Zraniteľné systémy:
Google Chrome 58.0.2987.133 a staršie

Odporúčania:
Odporúčame aktualizovať prehliadač Chrome na verziu 58.0.3029.81 alebo novšiu (v čase písania tohto prehľadu už je k dispozícii novšia verzia).

Zdroje:
https://chromereleases.googleblog.com/2017/04/stable-channel-update-for-desktop.html

4. Adobe Flash Player

Spoločnosť Adobe vydala opravy kritických zraniteľností v Adobe Flash Player a tiež jeho subkomponentoch ActionScript2 a SWF, ktoré umožňovali vzdialené vykonanie škodlivého kódu prostredníctvom zneužitia chýb v správe pamäti, ako napríklad použitie uvoľnenej pamäte a narušenie integrity pamäte.

Zraniteľné systémy:
Adobe Flash Player 25.0.0.127 a staršie

Odporúčania:
Čo najskôr aktualizovať Flash Player na verziu 25.0.0.148, nakoľko výskyt exploitov na uvedené zraniteľnosti je vysoko pravdepodobný. V závislosti od nastavení používateľa sa toto udeje automaticky alebo zobrazením dialógového okna s upozornením.

Zdroje:
https://helpx.adobe.com/security/products/flash-player/apsb17-10.html

6. Frameworky

Microsoft .NET

Spoločnosť Microsoft v apríli vydala opravu kritickej zraniteľnosti CVE-2017-0160, ktorá útočníkovi umožňuje zneužiť chybu vstupu pri načítavaní knižnice a získať možnosť vzdialeného vykonania škodlivého kódu, avšak, útočník by musel mať ešte predtým prístup ku lokálnemu systému.

Zraniteľné systémy:
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.5/3.5.1
Microsoft .NET Framework 4.5.2
Microsoft .NET Framework 4.6/4.6.1/4.6.2
Microsoft .NET Framework 4.7

Odporúčania:
Aplikovať aktualizácie distribuované prostredníctvom služby Windows Update. Pre zistenie čísla aktualizácie pre váš operačný systém a verziu .NET, navštívte nižšie uvedený odkaz.

Zdroje:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0160

Oracle Java

Spoločnosť Oracle v rámci aprílového balíka aktualizácií vydala opravu ôsmich zraniteľností, z toho troch kritických. Zraniteľnosti CVE-2017-3512 a CVE-2017-3514 v komponente AWT umožňovali útočníkovi vykonanie vzdialeného kódu, avšak s nevyhnutnosťou interakcie používateľa. Zraniteľnosť CVE-2017-3511 umožňuje lokálnemu útočníkovi povýšenie právomocí zneužitím chyby v komponente JCE pri načítavaní knižníc.

Zraniteľné systémy:
Java SE 6u141
Java SE 7u131
Java SE 8u121

Odporúčania:
Odporúčame aktualizovať na najnovšiu verziu Java SE 8u131. Aktualizácie sú dostupné prostredníctvom Java Auto Update, alebo na stránke www.java.com.

Zdroje:
http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html#AppendixJAVA
https://access.redhat.com/security/cve/cve-2017-3512
https://access.redhat.com/security/cve/cve-2017-3514

7. Iné závažné zraniteľnosti

Oracle VM VirtualBox

Spoločnosť Oracle vydala v rámci aprílových aktualizácií opravu pätnástich kritických zraniteľností v softvéri VirtualBox. Na šesť z týchto zraniteľností, umožňujúcich obídenie bezpečnostných opatrení a povýšenie oprávnení z hosťa na hostiteľa (guest-to-host) a tiež samotného používateľa na hostiteľskom systéme (host-user), existujú verejne dostupné exploity.

Zraniteľné systémy:
VM VirtualBox 5.0.38 a staršie
VM VirtualBox 5.1.20 a staršie

Odporúčania:
Čo najskôr aktualizovať na opravenú verziu (5.0.40 alebo 5.1.22), kvôli existencii verejne dostupných exploitov.

Zdroje:
http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html#AppendixOVIR

Oracle MySQL

V rámci aprílového balíka bolo pre rôzne komponenty vydaných štyridsať aktualizácií pre rôzne súčasti MySQL, z ktorých jedenásť môže byť zneužitých na diaľku. Najkritickejšou je oprava zero-day zraniteľnosti CVE-2017-5638, ktorá útočníkovi umožnila na diaľku vykonať škodlivý kód zneužitím chyby v Jakarta Multipart parseri (súčasť Apache Struts 2) pri uploade súboru. Za zmienku tiež

stojí zraniteľnosť CVE-2017-3599, na ktorú je exploit verejne známy a ktorá útočníkovi umožňuje zneužitím pretečenia integeru v subkomponente MySQL Server Pluggable Auth spôsobiť DoS útok, prípadne ďalšie bližšie nešpecifikované dopady.

Zraniteľné systémy:

MySQL Enterprise Monitor 3.1.6.8003 and staršie; 3.2.1182 and staršie; 3.3.2.1162 and staršie
MySQL Workbench 6.3.8 a staršie
MySQL Connectors 5.1.41 a staršie
MySQL Enterprise Backup 3.12.2 a staršie; 4.0.1 a staršie
MySQL Server 5.5.54 a staršie; 5.6.35 a staršie; 5.7.17 a staršie

Odporúčania:

Aplikovať aktualizácie čo najskôr, kvôli verejne dostupným a využívaným exploitom.

Zdroje:

http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html#AppendixMSQL
https://nvd.nist.gov/vuln/detail/CVE-2017-5638
https://nvd.nist.gov/vuln/detail/CVE-2017-3599

Uverejnenie exploitov od Equation Group

Skupina známa ako „Shadow Brokers“ uvoľnila tento mesiac balík prevažne útočných nástrojov od „Equation Group“, ktorý obsahuje exploity na niektoré produkty a platformy od spoločnosti Microsoft. Väčšina zraniteľností je údajne v podporovaných produktoch opravená. Spomenuté nástroje sú zamerané aj na zraniteľnosti v emailových serveroch a aplikáciách.

Zraniteľné systémy:

Windows Vista
Windows Vista Service Pack 2
Windows Vista x64 Edition Service Pack 2
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 x64-based Systems Service Pack 1
Windows 8.1 for 32-bit Systems
Windows 8.1 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 2003
Windows Server 2003 Service Pack 1
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

Ipswitch IMail Server 7.04 až 8.05
Ipswitch IMail Server 8.10 až 8.22
Internet Information Services 6.0
Avaya Call Server
IBM Lotus Domino 6.6.4 až 8.5.2
IBM Lotus Domino 6.5.4 a 7.0.2
IBM Lotus Notes
RedHat 7.0 až 7.1 Sendmail 8.11.x
MDaemon Messaging Server

Odporúčania:

Odporúčame aktualizovať produkty a zákazníkom používajúcim staršie systémy prejsť na novšie – podporované systémy. Pre zmiernenie rizika odporúča tiež zakázať nepotrebné alebo zastarané protokoly a komponenty (alebo aplikácie, ktoré ich používajú) (napr. SMBv1), použiť firewall, sledovať sieťovú komunikáciu a blokovať podozrivé komunikácie, a v organizáciách používať pre vzdialený prístup zamestnancov VPN.

Zdroje:

https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/
https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/shadow-brokers-leaks-hacking-tools-what-it-means-for-enterprises
https://success.trendmicro.com/solution/1117192