Mesačný prehľad kritických zraniteľností
Február 2017

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft v mesiaci február mimoriadne nevydala opravy žiadnych zraniteľností OS Windows. Plánovaný ferbruárový balík záplat by mal byť vydaný spolu s marcovými aktualizáciami. Boli však zverejnené opravy kritických zraniteľností integrovaného prehrávača Adobe Flash Player.

CERT/CC publikoval informácie ohľadom verejne známej zraniteľnosti CVE-2017-0016 v implementácie protokolu SMB. Zraniteľnosť umožňuje útočníkovi spôsobiť pád systému po pripojení sa ku škodlivému SMB serveru. Exploit na túto zraniteľnosť je verejne známy a doteraz nie je vydaná žiadna oprava tejto zraniteľnosti

Zraniteľné systémy:
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 RT 8.1
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016 for 64-bit Systems

Odporúčania:
Záplaty s novu verziou Adobe Flash Playera sú distribuované prostredníctvom bežného kanála Windows Update pod označením MS17-005. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré z uvedených zraniteľnosti Adobe Flash Playera je pravdepodobný.
Vzhľadom na 0-day zraniteľnosť CVE-2017-0016 s verejne známym exploitom odporúčame zablokovať spojenia protokolu SMB (TCP porty 139 a 445 a UDP porty 137 a 138) na zariadenia mimo lokálnej siete.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms17-005.aspx
https://blogs.technet.microsoft.com/msrc/2017/02/14/february-2017-security-update-release/
https://www.kb.cert.org/vuls/id/867968

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft v mesiaci február mimoriadne nevydala opravy žiadnych zraniteľností produktov Microsoft Office.

Zdroje:

https://blogs.technet.microsoft.com/msrc/2017/02/14/february-2017-security-update-release/

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft v mesiaci február mimoriadne nevydala opravy žiadnych zraniteľností prehliadača Microsoft Internet Explorer.

Zdroje:

https://blogs.technet.microsoft.com/msrc/2017/02/14/february-2017-security-update-release/

Microsoft Edge

Spoločnosť Microsoft v mesiaci február mimoriadne nevydala opravy žiadnych zraniteľností prehliadača Microsoft Edge.

Zdroje:

https://blogs.technet.microsoft.com/msrc/2017/02/14/february-2017-security-update-release/

Mozilla Firefox

Spoločnosť Mozilla vydala jednu aktualizáciu prehliadača Firefox opravujúcu 1 kritickú zraniteľnosť vo verzii pre OS Android, nevydala však žiadne opravy zraniteľností prehliadača Firefox pre iné platformy.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/mfsa2017-04/

Google Chrome

Spoločnosť Google zverejnila jednu aktualizácie prehliadača Chrome, ktoré neobsahuje opravy žiadnych bezpečnostných zraniteľností.

Zdroje:

https://googlechromereleases.blogspot.sk/2017/02/stable-channel-update-for-desktop.html

4. Adobe Flash Player

Spoločnosť Adobe zverejnila jednu aktualizáciu opravujúcu 13 zraniteľností, všetky sú označené ako kritické.

Zraniteľnosti sú spôsobené použitím opätovným použitím nesprávnych typov premenných, použitím uvoľnenej pamäte, pretečením pamäte, chybami pri práci s objektami v pamäti a ďalšími chybami. Tieto zraniteľnosti umožňujú vzdialenému útočníkovi spustiť škodlivý pomocou infikovaného Flash obsahu.

Zraniteľné systémy:
Adobe Flash Player verzie 24.0.0.194 a nižšej

Odporúčania:
Všetkým používateľom odporúčame aktualizovať Adobe Flash Player na verziu 24.0.0.221.
Aktualizáciu odporúčame vykonať čo najskôr, nakoľko boli exploity na niektoré uvedené zraniteľnosti publikované verejne.
Aktualizácie sú dostupné prostredníctvom stránky Adobe Flash Player Download Center, prípadne prostredníctvom kontroly dostupných aktualizácii v produkte Adobe Flash Player.

Zdroje:
https://helpx.adobe.com/security/products/flash-player/apsb17-04.html

5. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft v mesiaci február mimoriadne nevydala opravy žiadnych zraniteľností platformy Microsoft .NET.

Zdroje:
https://blogs.technet.microsoft.com/msrc/2017/02/14/february-2017-security-update-release/

Oracle Java

Spoločnosť Oracle v mesiaci február nevydala žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 18. apríl 2017.

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

6. Iné závažné zraniteľnosti

Zraniteľnosť DCCP v Linuxovom jadre

Zraniteľnosť CVE-2017-6074 je spôsobená dvojnásobným uvoľnením pamäte v implementácii DCCP (Datagram Congestion Control Protocol). Zraniteľnosť je možné zneužiť na lokálnu eskaláciu práv. Exploit na zraniteľnosť je verejne dostupný.

Zraniteľné systémy:
Linux Kernel verzie 4.9.11 a nižšej (jadrá skompilované od roku 2005 do 17.2.2017)

Odporúčania:
17.2.2017 bola zverejnená oprava uvedenej zraniteľnosti a postupne je distribuovaná s opravenými jadrami v hlavných Linuxových distribúciach. Administrátorom odporúčame čo najskôr aktualizovať jadro, nakoľko exploit na uvedenú zraniteľnosť je verejne dostupný.

Zdroje:
http://seclists.org/oss-sec/2017/q1/471
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-6074

Prakticky zneužiteľná kolízia v hashovacej funkcii SHA1

Výskumníci z Google a holandského CWI publikovali prvú prakticky zneužiteľnú kolíziu v hashovacej funkcii SHA1. Zároveň publikovali aj dvojicu PDF súborov s rôznym obsahom a rovnakým odtlačkom, na základe ktorej už vznikli verejne dostupné nástroje umožňujúce vytvárať takéto dvojice PDF súborov.

Odporúčania:
Správcom a vývojárom odporúčame preveriť, v ktorých systémoch používajú SHA1. Odporúčame prestať používať SHA1 a nahradiť ju bezpečnejšou funkciou, napr. SHA256

Zdroje:
https://shattered.io