Mesačný prehľad kritických zraniteľností
August 2016

1. Operačné systémy Microsoft Windows

Zraniteľnosti CVE-2016-3301, CVE-2016-3303 a CVE-2016-3304 v knižnici Windows font library sú spôsobená chybami pri spracovaní vložených fontov. Umožňujú vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení dokumentu obsahujúceho infikované vložené fonty. Útočník môže zneužitím týchto zraniteľností prevziať kontrolu nad zariadením.

Zraniteľnosť CVE-2016-3319 vo Windows PDF prehliadači je spôsobená chybami pri práci s objektmi v pamäti. Umožňuje vzdialené spustenie škodlivého kódu po otvorení infikovaného PDF súboru alebo po navštívení webstránky s infikovaným PDF obsahom.

Zraniteľnosť CVE-2016-3320 umožňuje pri zapnutej funkcii Secure Boot načítanie ľubovoľného zavádzača namiesto predinštalovaného Windows Boot Manager. Následne je možné vypnúť rôzne bezpečnostné mechanizmy systému Windows aj načítanie ľubovoľného operačného systému na zariadeniach so zapnutou funkciou Secure Boot. Na zneužitie tejto zraniteľnosti je potrebný administrátorský prístup k zariadeniu a preinštalovanie zavádzača Windows Boot Manager zraniteľnou verziou.

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 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 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for Itanium-based Systems Service Pack 2
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2

Windows Server 2012 R2 (Server Core installation)

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označeniami MS16-097, MS16-100 a MS16-102. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko použitie exploitov na niektoré zraniteľnosti je vysoko pravdepodobné.
Správcom systémov odporúčame prezrieť si augustové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-097.aspx
https://technet.microsoft.com/en-us/library/security/ms16-100.aspx
https://technet.microsoft.com/en-us/library/security/ms16-102.aspx

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosti CVE-2016-3313, CVE-2016-3316, CVE-2016-3317 a CVE-2016-33318 sú spôsobené chybami pri práci s objektmi v pamäti. Umožňujú vzdialené spustenie škodlivého kódu s právami prihláseného používateľa po otvorení infikovaného súboru (alebo zobrazení jeho náhľadu v emaile).

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 2013 RT Service Pack 1
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)

Microsoft Office for Mac 2011
Microsoft Office 2016 for Mac
Microsoft Word Viewer

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS16-099. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré uvedené zraniteľnosti je vysoko pravdepodobný.
Správcom systémov odporúčame prezrieť si augustový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-099.aspx

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na 9 zraniteľností, z ktorých je 5 označených ako kritických, sú spôsobené chybami pri práci s pamäťou a umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej stránky.

Zraniteľné systémy:

Microsoft Internet Explorer 9

Microsoft Internet Explorer 10

Microsoft Internet Explorer 11

Odporúčania:

Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS16-095. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si augustový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:

https://technet.microsoft.com/en-us/library/security/ms16-095.aspx

Microsoft Edge

Spoločnosť Microsoft vydala sadu záplat na 8 zraniteľností, z ktorých sú 4 označené ako kritické, sú spôsobené chybami pri práci s pamäťou a umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej stránky.

Zraniteľné systémy:

Microsoft Edge

Odporúčania:

Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS16-096. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedené zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si augustový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:

https://technet.microsoft.com/en-us/library/security/ms16-096.aspx

Mozilla Firefox

Spoločnosť Mozilla vydala jednu aktualizáciu prehliadača Firefox opravujúcu 4 kritické zraniteľnosti.

Zraniteľnosti CVE-2016-2835 a CVE-2016-2836 sú spôsobené bližšie nešpecifikovanými chybami pri práci s pamäťou a môžu viesť k vzdialenému spusteniu škodlivého kódu.

Zraniteľnosti CVE-2016-5258 a CVE-2016-5259 sú spôsobené opätovným použitím uvoľnenej pamäte pri práci s WebRTC, resp. Service Workers a môžu viesť ku vzdialenému spusteniu škodlivého kódu.

Zraniteľné systémy:
Mozilla Firefox 47.0.1 a predchádzajúce
Mozilla Firefox ESR 45.2 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 48 a Mozilla Firefox ESR 45.3).
Aktualizácia prehliadača by sa mala nainštalovať automaticky, pokiaľ sa tak nestalo, aktualizujte manuálne kliknutím na Firefox menu, ponuku Pomocníka a O prehliadači Firefox. Zobrazí sa okno s informáciou o používanej verzii prehliadača, súčasne sa skontrolujú a následne stiahnu aktualizácie.

Zdroje:
https://www.mozilla.org/sk/security/advisories/

Google Chrome

Spoločnosť Google zverejnila dve aktualizácie prehliadača Chrome, ktoré obsahujú opravy 43 bezpečnostných zraniteľností.

Najvážnejšie zraniteľnosti umožňujú spôsobiť pád aplikácie, XSS, url spoofing alebo iný, bližšie nešpecifikovaný dopad po načítaní infikovaných webstránok alebo zobrazovaní PDF súborov.

Zraniteľné systémy
Google Chrome do verzie 52.0.2743.116 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 53.0.2785.89. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://googlechromereleases.blogspot.sk/2016/08/stable-channel-update-for-desktop.html
http://googlechromereleases.blogspot.sk/2016/08/stable-channel-update-for-desktop_31.html

4. Adobe Flash Player

Spoločnosť Adobe v mesiaci august nezverejnila žiadnu aktualizáciu prehrávača Adobe Flash Player.

Zdroje:
https://helpx.adobe.com/security.html#flashplayer

5. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft v mesiaci august nezverejnila opravy žiadnych zraniteľností platformy .NET.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-aug.aspx

Oracle Java

Spoločnosť Oracle v mesiaci august nevydala žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 18. október 2016.

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

6. Iné závažné zraniteľnosti

Exploity na viaceré zraniteľnosti sieťových prvkov

Boli verejne publikované viaceré exploity a nástroje používané skupinou Equation Group na kompromitáciu firewallov. Obsiahnuté exploity sú zamerané okrem iného na zariadenia od výrobcov Cisco (ASA, PIX, FWSM) a Fortigate a umožňujú úplnú kompromitáciu daných zariadení. So získaným správcovským prístupom ku kompromitovaným firewallom sú možné ďalšie útoky ako napríklad: MITM, prienik do chránenej siete, DoS, data sniffing a podobne. Bližší popis jednotlivých zraniteľností aj zraniteľných verzií je dostupný na odkazoch nižšie.

Vzhľadom na uvedené riziká odporúčame používateľom, ktorí majú vo svojej sieti zraniteľné zariadenia:

- firmware/OS upgrade opravujúci nájdené zraniteľnosti
- overiť integritu zraniteľných zariadení
- zariadenia Cisco PIX a FWSM už nie sú podporované - mali by byť vyradené z prevádzky a nahradené podporovanými zariadeniami
- konfigurácia manažment prístupu: uistiť sa, že správcovské rozhrania firewallov sú prístupné len z manažmentových sietí a nie z rozhraní pripojených do externých sietí

- konfigurácia SNMP: uistiť sa, že nie sú použité default alebo jednoduché community reťazce; že sú špecifikované len autorizované SNMP servery; SNMP je povolené len na potrebných rozhraniach

Zdroje:
http://blogs.cisco.com/security/shadow-brokers
http://fortiguard.com/advisory/FG-IR-16-023
http://cert.europa.eu/static/SecurityAdvisories/CERT-EU-SA2016-133.txt