Mesačný prehľad kritických zraniteľností
Jún 2016

1. Operačné systémy Microsoft Windows

Zraniteľnosti CVE-2016-3205, CVE-2016-3206 a CVE-2016-3207 skriptovacieho enginu VBScript a JScript sú spôsobené chybami pri práci s objektmi v pamäti. Umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej webovej stránky.

Zraniteľnosť CVE-2016-3227 Windows DNS Servera je spôsobené chybami pri spracovaní DNS dopytov. Útočník môže túto zraniteľnosť zneužiť na vzdialené spustenie škodlivého kódu so systémovými právami odoslaním škodlivého DNS dopytu na server.

Zraniteľnosti CVE-2016-3213 a CVE-2016-3236 vo Windows Web Proxy Auto Discovery (WPAD) sú spôsobené nesprávnym spracovaním niektorých scenárov použitia protokolu WPAD. Umožňujú útočníkovi zvýšiť oprávnenia a kontrolovať sieťovú prevádzku v internej sieti organizácií. Na zneužitie zraniteľnosti stačí napr. navštívenie infikovanej webovej stránky. Zraniteľnosť je známa aj pod označením „BadTunnel“.

Zraniteľnosť CVE-2016-3203 vo Windows PDF prehliadači umožňuje vzdialené spustenie škodlivého kódu po otvorení infikovaného PDF súboru.

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 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 MS16-069, MS16-071, MS16-077, MS-16-080 a taktiež aj MS16-083, ktorá obsahuje najnovšiu verziu Adobe Flash Player. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko použitie exploitov na niektoré zraniteľnosti je vysoko pravdepodobné.

Správcom systémov odporúčame prezrieť si júnové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:

https://technet.microsoft.com/en-us/library/security/ms16-069.aspx
https://technet.microsoft.com/en-us/library/security/ms16-071.aspx
https://technet.microsoft.com/en-us/library/security/ms16-077.aspx
https://technet.microsoft.com/en-us/library/security/ms16-080.aspx
https://technet.microsoft.com/en-us/library/security/ms16-083.aspx
https://nakedsecurity.sophos.com/2016/06/16/badtunnel-a-vulnerability-all-windows-users-need-to-patch/

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosti CVE-2016-0025 a CVE-2016-3233 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 emaili).

Zraniteľnosť CVE-2016-3235 je spôsobená nesprávnou kontrolou načítavaných DLL súborov a umožňuje útočníkovi podvrhnúť škodlivé DLL, prostredníctvom ktorého je možné spustiť škodlivý kód pri otvorení dokumentu MS Office.

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
Microsoft Visio Viewer 2007 Service Pack 3
Microsoft Visio Viewer 2010 (32-bit editions)
Microsoft Visio Viewer 2010 (64-bit editions)
Microsoft Office Compatibility Pack Service Pack 3

Microsoft SharePoint Server 2010 Service Pack 2
Microsoft SharePoint Server 2013 Service Pack 1
Microsoft Office Web Apps 2010 Service Pack 2
Microsoft Office Web Apps 2013 Service Pack 1

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS16-070. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedené zraniteľnosti je vysoko pravdepodobný.
Správcom systémov odporúčame prezrieť si júnové Microsoft Security Bulletin dostupné na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-070.aspx

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na 10 zraniteľností, z ktorých je 7 označených ako kritických, sú spôsobené chybami pri práci s pamäťou a umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej stránky. Bolo zaznamenané zneužitie zraniteľnosti CVE-2016-0189 útočníkmi.

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 MS16-063. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si júnový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-063.aspx

Microsoft Edge

Spoločnosť Microsoft vydala sadu záplat na 8 zraniteľností, z ktorých je 5 označených ako kritických, sú spôsobené chybami pri práci s pamäťou alebo pri spracovávaní PDF súborov a umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej stránky alebo zobrazení infikovaného PDF súboru.

Zraniteľné systémy:
Microsoft Edge

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS16-068. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedené zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si júnovový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-068.aspx

Mozilla Firefox

Spoločnosť Mozilla vydala jednu aktualizáciu prehliadača Firefox opravujúcu 3 kritické zraniteľnosti.

Zraniteľnosti CVE-2016-2815 a CVE-2016-2818 sú spôsobené bližšie nešpecifikovanými chybami pri práci s pamäťou a môžu viesť k vzdialenému spusteniu škodlivého kódu.

Zraniteľnosť CVE-2016-2819 je spôsobená pretečením pamäte pri spracovaní HTML5 fragmentov a môže viesť ku vzdialenému spusteniu škodlivého kódu.

Zraniteľné systémy:
Mozilla Firefox 46.0.1 a predchádzajúce
Mozilla Firefox ESR 45.1.1 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 47 a Mozilla Firefox ESR 45.2).
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 styri aktualizácie prehliadača Chrome, ktoré obsahujú opravy 18 bezpečnostných zraniteľností.

Najvážnejšie zraniteľnosti umožňujú spôsobiť pád aplikácie, XSS, únik informácií alebo iný, bližšie nešpecifikovaný dopad po načítaní infikovaných webstránok.

Zraniteľné systémy
Google Chrome do verzie 51.0.2704.84 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 51.0.2704.103, resp. 51.0.2704.106. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://googlechromereleases.blogspot.sk/2016/06/stable-channel-update.html
http://googlechromereleases.blogspot.sk/2016/06/stable-channel-update_6.html
http://googlechromereleases.blogspot.sk/2016/06/stable-channel-update_16.html
http://googlechromereleases.blogspot.sk/2016/06/stable-channel-update_23.html

4. Adobe Flash Player

Spoločnosť Adobe zverejnila jednu aktualizáciu opravujúcu 36 zraniteľností, všetky sú označené ako kritické.

Zraniteľnosti sú spôsobené použitím nesprávnych typov premenných, opätovným použitím uvoľnenej pamäte, chybami pri práci s objektami v pamäti, pretečením pamäte (heap buffer overflow) a a nesprávnou kontrolou pri načítavaní DLL knižníc. Tieto zraniteľnosti umožňujú vzdialenému útočníkovi spustiť škodlivý kód pomocou infikovaného Flash obsahu.
Bolo zaznamenané aktívne zneužívanie zraniteľnosti CVE-2016-4171.

Zraniteľné systémy:
Adobe Flash Player verzie 21.0.0.242 a nižšej
Adobe Flash Player verzie 18.0.0.352 a nižšej
Adobe Flash Player verzie 11.2.202.621 a nižšej

Odporúčania:
Používateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 22.0.0.192, používateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu 18.0.0.360. Používateľom Linux odporúčame aktualizovať na verziu 11.2.202.626.
Aktualizáciu odporúčame vykonať čo najskôr, nakoľko exploity na niektoré zraniteľnosti sú už používané.
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/apsa16-03.html
https://helpx.adobe.com/security/products/flash-player/apsb16-18.html

5. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft v mesiaci máj nevydala opravy žiadnych zraniteľností platformy .NET.

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

Oracle Java

Spoločnosť Oracle v mesiaci jún nevydala žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 19. júl 2016.
Zdroje:
http://www.oracle.com/technetwork/topics/security/alerts-086861.html

6. Iné závažné zraniteľnosti

Linux Privilege Escalation

Spoločnosť Google publikovala informácie o zraniteľnosti v jadre OS Linux, ktorú je možné zneužiť na eskaláciu privilégií (získanie administrátorských práv). Zraniteľnosť je spôsobená pretečením zásobníka využívaného v jadre pri systémových volaniach. Táto zraniteľnosť môže byť zneužitá napr. prostredníctvom súborového systému ecryptfs. Ukážkový exploit je verejne dostupný.

Zraniteľné systémy:
Linux Kernel verzie staršie ako z 10. júna 2016

Odporúčania:
Boli zverejnené dve záplaty Linuxového jadra, odporúčame čo najskôr aktualizovať jadro na najnovšiu dostupnú verziu, keďže exploit aj podrobný popis zraniteľnosti je verejne známy.

Zdroje:
http://googleprojectzero.blogspot.sk/2016/06/exploiting-recursion-in-linux-kernel_20.html

NTPd

V referenčnej implementácii NTP servera NTPd boli nájdené zraniteľnosti, ktoré umožňujú vzdialeným útočníkom odoslať NTP serveru škodlivé packety a spôsobiť tak jeho pád a následné rozsynchronizovanie lokálnych hodín v jednotlivých zariadeniach, čo môže uľahčiť vykonanie rôznych útokov založených na časovaní.

Zraniteľné systémy:
NTPd do verzie 4.2.8p8

Odporúčania:
Odporúčame aktualizovať NTPd server na verziu 4.2.8p8. V prípade, že aktualizácia nie je dostupná, alebo ju nie je možné vykonať, odporúčame aplikovať aspoň nasledovné opatrenia:

- Implementovať BCP-38
- Monitorovať činnosť ntpd

Zdroje:

https://www.kb.cert.org/vuls/id/321640
http://support.ntp.org/bin/view/Main/NtpBug3042
http://support.ntp.org/bin/view/Main/NtpBug3043
http://support.ntp.org/bin/view/Main/NtpBug3044
http://support.ntp.org/bin/view/Main/NtpBug3045
http://support.ntp.org/bin/view/Main/NtpBug3046