Mesačný prehľad kritických zraniteľností
Apríl 2016

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2016-0145 v knižnici Windows font library je spôsobená chybami pri spracovaní fontov vložených v dokumentoch. Umožňuje vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení dokumentu obsahujúceho infikované vložené fonty. Útočník môže zneužitím tejto zraniteľnosti získať systémové práva a prevziať kontrolu nad zariadením.

Zraniteľnosti CVE-2016-0165 a CVE-2016-0167 vo Windows Kernel Mode Drivers v komponente Win32k sú spôsobené chybami pri práci s objektmi v pamäti. Umožňujú prihláseným používateľom získať oprávnenia systémového používateľa a prevziať kontrolu nad zariadením. Bolo zaznamenané zneužitie týchto zraniteľností útočníkmi.

Zraniteľnosť CVE-2016-0147 v komponente Microsoft XML Core je spôsobená chybou pri spracovaní používateľského vstupu. Umožňuje vzdialené spustenie škodlivého kódu po navštívení webstránky využívajúcej MS XML. Útočník môže zneužitím tejto zraniteľnosti získať systémové práva a prevziať kontrolu nad zariadením.

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 MS16-039, MS-040 a taktiež aj MS16-050 obsahujúca najnovšiu verziu Adobe Flash Player. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko bolo zaznamenané použitie exploitov na niektoré zraniteľnosti.
Správcom systémov odporúčame prezrieť si aprílové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-039.aspx
https://technet.microsoft.com/en-us/library/security/ms16-040.aspx
https://technet.microsoft.com/en-us/library/security/ms16-050.aspx

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosť CVE-2016-0127 je spôsobená chybami pri práci s objektmi v pamäti. Umožňuje vzdialené spustenie škodlivého kódu s právami prihláseného používateľa po otvorení infikovaného súboru (alebo zobrazení jeho náhľadu v emaili).

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 Excel Viewer
Microsoft Office Compatibility Pack Service Pack 3

Microsoft SharePoint Server 2007 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 MS16-042. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedené zraniteľnosti je pravdepodobný.

Správcom systémov odporúčame prezrieť si aprílové Microsoft Security Bulletin dostupné na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-042.aspx

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na 6 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 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 MS16-037. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si aprílový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-037.aspx

Microsoft Edge

Spoločnosť Microsoft vydala sadu záplat na 6 zraniteľnosti, 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 MS16-038. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedené zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si aprílový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-038.aspx

Mozilla Firefox

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

Zraniteľnosti CVE-2016-2804, CVE-2016-2805, CVE-2016-2806 a CVE-2016-2807 sú spôsobené bližšie nešpecifikovanými chybami pri práci s pamäťou môžu viesť k vzdialenému spusteniu škodlivého kódu.

Zraniteľné systémy:
Mozilla Firefox 45.0.2 a predchádzajúce
Mozilla Firefox ESR 38.7.1 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 46 a Mozilla Firefox ESR 45.1, resp. Mozilla Firefox ESR 38.8).
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 štyri aktualizácie prehliadača Chrome, ktoré obsahujú opravy 29 bezpečnostných zraniteľností.

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

Zraniteľné systémy
Google Chrome do verzie 50.0.2661.87 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 50.0.2661.94. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://googlechromereleases.blogspot.sk/2016/04/stable-channel-update.html
http://googlechromereleases.blogspot.sk/2016/04/stable-channel-update_13.html
http://googlechromereleases.blogspot.sk/2016/04/stable-channel-update_20.html
http://googlechromereleases.blogspot.sk/2016/04/stable-channel-update_28.html

4. Adobe Flash Player

Spoločnosť Adobe zverejnila jednu aktualizáciu opravujúcu 24 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 zásobníka, pretečením rozsahu celých čísel a ďalšími chybami. Tieto zraniteľnosti umožňujú vzdialenému útočníkovi spustiť škodlivý kód pomocou infikovaného Flash obsahu.
Bolo zaznamenané aktívne zneužívanie zraniteľnosti CVE-2016-1019.

Zraniteľné systémy:
Adobe Flash Player verzie 21.0.0.197 a nižšej
Adobe Flash Player verzie 18.0.0.333 a nižšej
Adobe Flash Player verzie 11.2.202.577 a nižšej

Odporúčania:
Používateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 21.0.0.213, používateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu 18.0.0.343. Používateľom Linux odporúčame aktualizovať na verziu 11.2.202.616.
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/apsa16-01.html
https://helpx.adobe.com/security/products/flash-player/apsb16-10.html

5. Frameworky

Microsoft .NET Framework

Zraniteľnosť CVE-2016-0145 v knižnici Windows font library je spôsobená chybami pri spracovaní fontov vložených v dokumentoch. Umožňuje vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení dokumentu obsahujúceho infikované vložené fonty. Útočník môže zneužitím tejto zraniteľnosti získať systémové práva a prevziať kontrolu nad zariadením.

Zraniteľnosť CVE-2016-1148 spôsobená nesprávnou kontrolou pri načítaní dynamických knižníc umožňuje útočníkovi podvrhnúť vlastnú DLL knižnicu so škodlivým kódom namiesto knižnice poskytnutej operačným systémom. Zneužitím zraniteľnosti je možné spustiť škodlivý kód po otvorení súboru z adresára (napr. na zdieľanom disku), ktorý obsahuje aj infikovanú DLL knižnicu.

Zraniteľné systémy:
Microsoft .NET Framework 3.0 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

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS16-039 a MS16-041. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér. Správcom systémov odporúčame prezrieť si aprílový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-039.aspx
https://technet.microsoft.com/en-us/library/security/ms16-041.aspx

Oracle Java

Spoločnosť Oracle v mesiaci január vydala bezpečnostnú aktualizáciu platformy Java opravujúcu 9 zraniteľností, z ktorých je 5 kritických.

Zraniteľnosti CVE-2016-0686, CVE-2015-0687, CVE-2015-3427, CVE-2015-3443 a CVE-2016-3449 umožňujú vzdialenému útočníkovi bez autentifikácie spustenie škodlivého kódu, kompromitáciu zariadenia, alebo iné bližšie neurčené dopady.

Zraniteľné systémy:
Java SE 6u113
Java SE 7u99
Java SE 8u77

Odporúčania:
Spoločnosť Oracle zverejnila aktualizáciu prostredníctvom bežného kanála Java Auto Update. Aktualizácie sú dostupné aj na stránke java.com. Používateľom odporúčame nainštalovať najnovšiu verziu Java SE 8 Update 91.

Zdroje:
http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html

6. Iné závažné zraniteľnosti

Badlock

Zraniteľnosť týkajúca sa OS Windows (CVE-2016-0128) aj Samba (CVE-2016-2118) umožňujúca spôsobiť útok typu zamietnutie služby (DoS), prípadne pri útoku typu Man-in-the-Middle (MitM) môže dosiahnuť eskaláciu práv a vykonávať akcie v mene prihláseného používateľa. Útočník však musí byť schopný kontrolovať a modifikovať prevádzku v sieti, aby mohol vykonať MitM útok.

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS16-047. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér. Správcom systémov odporúčame prezrieť si aprílový Microsoft Security Bulletin dostupný na odkaze nižšie.
Vývojári Samby taktiež zverejnili aktualizácie, odporúčame čo najskôr aktualizovať softvér na niektorú z verzií 4.2.10, 4.2.11, 4.3.7, 4.3.8, 4.4.1, 4.4.2.

Zdroje:
http://badlock.org/
https://technet.microsoft.com/en-us/library/security/ms16-047.aspx