Mesačný prehľad kritických zraniteľností
Marec 2016

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2016-0121 v knižnici Adobe Type Manager 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-2016-0098 a CVE-2016-0101 operačného systému Microsoft Windows sú spôsobená chybami pri spracovaní multimediálneho obsahu. Umožňujú vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení infikovaného súboru. Útočník môže zneužitím týchto zraniteľností získať systémové práva a prevziať kontrolu nad zariadením.

Zraniteľnosti CVE-2016-0117 a CVE-2016-0118 operačného systému Microsoft Windows sú spôsobená chybami pri práci s .pdf súbormi. Umožňujú 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 MS16-026, MS-027, MS16-028 a taktiež aj MS16-036 obsahujáca najnovšiu verziu Adobe Flash Player. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko použitie exploitov na niektoré zraniteľnosti je pravdepodobné.
Správcom systémov odporúčame prezrieť si marcové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-026.aspx
https://technet.microsoft.com/en-us/library/security/ms16-027.aspx
https://technet.microsoft.com/en-us/library/security/ms16-028.aspx
https://technet.microsoft.com/en-us/library/security/ms16-036.aspx

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft v mesiaci marec nevydala opravy žiadnych kritických zraniteľností Microsoft Office. Boli však zverejnené dôležité aktualizácie opravujúce zraniteľnosti umožňujúce vzdialené spustenie kódu alebo obídenie bezpečnostných mechanizmov.

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 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 MS16-029. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedené zraniteľnosti je pravdepodobný.

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

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-029.aspx

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na 13 zraniteľností, všetkých 13 je 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 MS16-023. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si marcový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-023.aspx

Microsoft Edge

Spoločnosť Microsoft vydala jednu sadu záplat na 11 zraniteľnosti, z ktorých je 10 označených ako kritických, 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 MS16-024. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedené zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si marcový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-024.aspx

Mozilla Firefox

Spoločnosť Mozilla vydala jednu aktualizáciu prehliadača Firefox opravujúce 23 kritických zraniteľností.

Dokopy 15 zraniteľností v knižnici Graphite 2 je spôsobených prevažne chybami pri práci s pamäťou a môžu byť zneužité na vzdialené spustenie škodlivého kódu prostredníctvom infikovaných fontov.

Zraniteľnosť CVE-2016-1950 v knižnici NSS je spôsobená pretečením pamäte (heap-based buffer overflow) pri spracovaní ASN.1 štruktúr a môže byť zneužitá na vzdialené spustenie škodlivého kódu prostredníctvom infikovaného certifikátu.

Zraniteľnosť CVE-2016-1964 je spôsobená opätovným použitím uvoľnenej pamäte pri práci s XML a môže byť zneužitá na vzdialené spustenie škodlivého kódu prostredníctvom webstránky s infikovaným obsahom.

Zraniteľnosť CVE-2016-1962 je spôsobená opätovným použitím uvoľnenej pamäte pri používaní viacnásobných WebRTC spojení a môže byť zneužitá na vzdialené spustenie škodlivého kódu prostredníctvom uvoľnenia aktíveho spojenia.

Zraniteľnosti CVE-2016-1960 a CVE-2016-1961 sú spôsobené opätovným použitím uvoľnenej pamäte pri spracovaní HTML dokumentov a môžu byť zneužité na vzdialené spustenie škodlivého kódu prostredníctvom infikovanej webstránky, resp. SVG obrázku.

Zraniteľnosť CVE-2016-1959 je spôsobená čítaním mimo hraníc v ServiceWorkermanager a môže byť zneužitá na vzdialené spustenie škodlivého kódu bližšie neurčeným spôsobom.

Zraniteľnosti CVE-2016-1952 a CVE-2016-1953 spôsobené bližšie nešpecifikovanými chybami pri práci s pamäťou môžu viesť k vzdialenému spusteniu škodlivého kódu.

Zraniteľné systémy:
Mozilla Firefox 44.0.2 a predchádzajúce
Mozilla Firefox ESR 38.6.1 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 45.0.1 a Mozilla Firefox ESR 38.7)
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 34 bezpečnostných zraniteľností.

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

Zraniteľné systémy
Google Chrome do verzie 49.0.2623.87 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 49.0.2623.108, prípadne 49.0.2623.110. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://googlechromereleases.blogspot.sk/2016/03/stable-channel-update.html
http://googlechromereleases.blogspot.sk/2016/03/stable-channel-update_8.html
http://googlechromereleases.blogspot.sk/2016/03/stable-channel-update_24.html
http://googlechromereleases.blogspot.sk/2016/03/stable-channel-update_28.html

4. Adobe Flash Player

Spoločnosť Adobe zverejnila jednu aktualizáciu opravujúcu 23 zraniteľností, všetky sú označené ako kritické.

Zraniteľnosti sú spôsobené opätovným použitím uvoľnenej pamäte, pretečením pamäte, 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-2016-1010 v cielených útokoch.

Zraniteľné systémy:
Adobe Flash Player verzie 20.0.0.306 a nižšej
Adobe Flash Player verzie 18.0.0.329 a nižšej
Adobe Flash Player verzie 11.2.202.569 a nižšej

Odporúčania:
Používateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 21.0.0.182, používateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu 18.0.0.333. Používateľom Linux odporúčame aktualizovať na verziu 11.2.202.577.
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/apsb16-08.html

5. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft v mesiaci marec nevydala opravy žiadnych kritických zraniteľností platformy .NET. Boli však zverejnené dôležité aktualizácie opravujúce zraniteľnosti validácie podpísaných XML dokumentov, ktoré umožňovali vytvoriť modifikovaný XML dokument s „platným“ podpisom.

Zraniteľné systémy:
Microsoft .NET Framework 2.0 Service Pack 2
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 MS16-035. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér. Správcom systémov odporúčame prezrieť si februárový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-035.aspx

Oracle Java

Najbližšia veľká sada aktualizácií je naplánovaná na 19. apríl 2016. Spoločnosť Oracle však v mesiaci marec vydala jednu aktualizácie platformy Java opravujúcu kritickú zraniteľnosť CVE-2016-0636, ktorá môže byť zneužitá na diaľku bez použitia prihlasovacích údajov a umožňuje spôsobiť pád systému, únik informácií a ďalšie bližšie nešpecifikované dopady napr. po navštívení infikovanej webstránky.

Zraniteľné systémy:
Java SE 7u97
Java SE 8u73, 8u74

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 77.

Zdroje:
http://www.oracle.com/technetwork/topics/security/alert-cve-2016-0636-2949497.html