Mesačný prehľad kritických zraniteľností
September 2016

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2016-3356 vo Windows GDI je spôsobená chybami pri práci s objektmi v pamäti. Umožňuje vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení infikovaného dokumentu. Útočník môže zneužitím tejto zraniteľnosti prevziať kontrolu nad zariadením.

Zraniteľnosť CVE-2016-3375 v Microsoft OLE Automation a v skriptovacom engine VBScript je spôsobená chybami pri prístupe k objektom v pamäti. Umožňuje vzdialené spustenie škodlivého kódu po navštívení infikovanej webovej stránky.

Zároveň boli opravené viaceré ďalšie zraniteľnosti spôsobené chybami ovládačov v jadre systému pri práci s objektami v pamäti. Tieto zraniteľnosti umožňujú eskaláciu privilégií prihláseným používateľom a získanie administrátorských oprávnení po spustení škodlivých programov.

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 MS16-106, MS16-116 a taktiež aj MS16-117, 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 septembrové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-106.aspx
https://technet.microsoft.com/en-us/library/security/ms16-116.aspx
https://technet.microsoft.com/en-us/library/security/ms16-117.aspx

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosti CVE-2016-3357, CVE-2016-3358, CVE-2016-3359, CVE-2016-3360, CVE-2016-3361, CVE-2016-3362, CVE-2016-3363, CVE-2016-3364, CVE-2016-3365 a CVE-2016-3381 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
Microsoft Excel Viewer
Microsoft PowerPoint Viewer
Microsoft Office Compatibility Pack Service Pack 3

Microsoft SharePoint Server 2010 Service Pack 2
Microsoft SharePoint Server 2013 Service Pack 1
Microsoft SharePoint Server 2016
Microsoft Office Web Apps 2010 Service Pack 2
Microsoft Office Web Apps 2013 Service Pack 1
Office Online Server

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS16-107. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré uvedené zraniteľnosti je pravdepodobný.
Správcom systémov odporúčame prezrieť si septembrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-107.aspx

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na 10 zraniteľností, z ktorých sú 2 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 MS16-104. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si septembrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-104.aspx

Microsoft Edge

Spoločnosť Microsoft vydala sadu záplat na 12 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 MS16-105. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedené zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si septembrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-105.aspx

Mozilla Firefox

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

Zraniteľnosť CVE-2016-5275 je spôsobená pretečením pamäte pri použití prázdnych filtrov počas renderovania elementu canvas a môže viesť ku vzdialenému spusteniu škodlivého kódu.

Zraniteľnosť CVE-2016-5278 je spôsobená pretečením pamäte pri enkódovaní obrázkov a môže viesť ku vzdialenému spusteniu škodlivého kódu.

Zraniteľnosti CVE-2016-5256 a CVE-2016-5257 sú spôsobené bližšie nešpecifikovanými chybami pri práci s pamäťou a môžu viesť k vzdialenému spusteniu škodlivého kódu.

Zraniteľné systémy:
Mozilla Firefox 48.0.2 a predchádzajúce
Mozilla Firefox ESR 45.3 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 49 a Mozilla Firefox ESR 45.4).
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/en-US/security/advisories/mfsa2016-85/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-86/

Google Chrome

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

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

Zraniteľné systémy
Google Chrome do verzie 53.0.2785.116 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 53.0.2785.143. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
https://googlechromereleases.blogspot.sk/2016/09/stable-channel-update-for-desktop.html
https://googlechromereleases.blogspot.sk/2016/09/stable-channel-update-for-desktop_13.html
https://googlechromereleases.blogspot.sk/2016/09/stable-channel-update-for-desktop_14.html
https://googlechromereleases.blogspot.sk/2016/09/stable-channel-update-for-desktop_29.html

4. Adobe Flash Player

Spoločnosť Adobe zverejnila jednu aktualizáciu opravujúcu 26 zraniteľností, všetky sú označené ako kritické.

Zraniteľnosti sú spôsobené pretečením rozsahu celých čísel, opätovným použitím uvoľnenej pamäte, chybami pri práci s objektami v pamäti a ďalšími chybami. Tieto zraniteľnosti umožňujú vzdialenému útočníkovi spustiť škodlivý kód alebo únik informácií pomocou infikovaného Flash obsahu.

Zraniteľné systémy:
Adobe Flash Player verzie 22.0.0.211 a nižšej
Adobe Flash Player verzie 18.0.0.366 a nižšej
Adobe Flash Player verzie 11.2.202.632 a nižšej

Odporúčania:
Používateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 23.0.0.162, používateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu 18.0.0.375. Používateľom Linux odporúčame aktualizovať na verziu 11.2.202.635.
Aktualizáciu odporúčame vykonať čo najskôr, nakoľko je výskyt exploitov na niektoré uvedené zraniteľnosti vysoko pravdepodobný.
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/apsb16-29.html

5. Frameworky

Microsoft .NET Framework

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

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

Oracle Java

Spoločnosť Oracle v mesiaci september 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

Kritické zraniteľnosti v MySQL

Boli zverejnené informácie o dvoch kritických zraniteľnostiach v databázach MySQL umožňujúce zápis do konfiguračných súborov, prostredníctvom ktorého je následne možné dosiahnuť načítanie ľubovoľných knižníc a spustenie škodlivého kódu. Pôvodne boli zraniteľnosti publikované ako 0-day, ale v čase ich publikácie už boli vydané opravené verzie MySQL.

Zraniteľné systémy:
MySQL do verzie 5.7.14 (vrátane)
MySQL do verzie 5.6.32 (vrátane)
MySQL do verzie 5.5.51 (vrátane)

Odporúčania:
Správcom MySQL odporúčame aktualizovať softvér na aktuálnu verziu 5.7.15, 5.6.33, resp. 5.5.52.

Zdroje:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6662