Mesačný prehľad kritických zraniteľností
Máj 2016

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2016-0189 skriptovacieho enginu VBScript a JScript je spôsobená chybami pri práci s objektmi v pamäti. Umožňuje vzdialené spustenie škodlivého kódu po navštívení infikovanej webovej stránky. Bolo zaznamenané zneužitie tejto zraniteľnosti útočníkmi.

Zraniteľnosti CVE-2016-0170, CVE-2016-0184 a CVE-2016-0195 vo Windows GDI, Direct3D a Windows Imaging Component sú spôsobené chybami pri práci s objektmi v pamäti. Umožňuje vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení infikovaného dokumentu. Útočník môže zneužitím tejto zraniteľnosti získať systémové práva a prevziať kontrolu nad zariadením. Bolo zaznamenané zneužitie zraniteľnosti CVE-2016-0184 útočníkmi.

Zraniteľnosť CVE-2016-0182 aplikácie Windows Denník (Journal) je spôsobená chybou pri spracovaní súborov Windows Denník (.jnt) a umožňuje vzdialené spustenie škodlivého kódu po otvorení infikovaného súboru Windows Denník.

Zraniteľnosť CVE-2016-0179 v používate+skom rozhraní Windows Shell je spôsobená chybami pri práci s objektmi v pamäti. Umožňuje vzdialené spustenie škodlivého kódu po navštívení webstránky. 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 MS16-053, MS-055, MS-056, MS-057 a taktiež aj MS16-064, ktorá obsahuje 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 májové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-053.aspx
https://technet.microsoft.com/en-us/library/security/ms16-055.aspx
https://technet.microsoft.com/en-us/library/security/ms16-056.aspx
https://technet.microsoft.com/en-us/library/security/ms16-057.aspx
https://technet.microsoft.com/en-us/library/security/ms16-064.aspx

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosť CVE-2016-0183 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-2016-0198 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 Office Compatibility Pack Service Pack 3

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

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS16-054. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedené zraniteľnosti je pravdepodobný.
Správcom systémov odporúčame prezrieť si májové Microsoft Security Bulletin dostupné na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-054.aspx

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na 5 zraniteľností, z ktorých sú 3 označené ako kritické, 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 MS16-051. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko bol zaznamenaný výskyt exploitov na niektoré zraniteľnosti. Správcom systémov odporúčame prezrieť si májový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-051.aspx

Microsoft Edge

Spoločnosť Microsoft vydala sadu záplat na 4 zraniteľnosti, z ktorých sú všetky 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

MS16-052. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedené zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si májový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-052.aspx

Mozilla Firefox

Spoločnosť Mozilla nevydala v mesiaci máj žiadnu aktualizáciu prehliadača Firefox.

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

Google Chrome

Spoločnosť Google zverejnila dve aktualizácie prehliadača Chrome, ktoré obsahujú opravy 47 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 50.0.2661.102 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 51.0.2704.63. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://googlechromereleases.blogspot.sk/2016/05/stable-channel-update.html
http://googlechromereleases.blogspot.sk/2016/05/stable-channel-update_25.html

4. Adobe Flash Player

Spoločnosť Adobe zverejnila jednu aktualizáciu opravujúcu 27 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 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-2016-4117.
Zraniteľnosť CVE-2016-4116 bola identifikovaná tímom CSIRT.SK.

Zraniteľné systémy:
Adobe Flash Player verzie 21.0.0.226 a nižšej
Adobe Flash Player verzie 18.0.0.343 a nižšej
Adobe Flash Player verzie 11.2.202.616 a nižšej

Odporúčania:
Používateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 21.0.0.242, používateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu 18.0.0.352. Používateľom Linux odporúčame aktualizovať na verziu 11.2.202.621.
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/apsa16-02.html
https://helpx.adobe.com/security/products/flash-player/apsb16-15.html
http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=147

5. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft v mesiaci máj nevydala opravy žiadnych kritických zraniteľností platformy .NET. Bola však zverejnená dôležitá aktualizácia opravujúca zraniteľnosť v implementácii TLS/SSL protokolu v .NET komponente pre šifrovanie. Útočník môže zneužiť túto zraniteľnosť na vykonanie Man-in-the-middle útoku a dešifrovať komunikáciu.

Zraniteľné systémy:
Microsoft .NET Framework 2.0 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 MS16-065. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér. Správcom systémov odporúčame prezrieť si májový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-065.aspx

Oracle Java

Spoločnosť Oracle v mesiaci február 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

Adobe Acrobat a Reader

Spoločnosť Adobe zverejnila jednu aktualizáciu opravujúcu 93 zraniteľností, všetky sú označené ako kritické.

Zraniteľnosti sú spôsobené použitím opätovným použitím uvoľnenej pamäte, chybami pri práci s pamäťou, pretečením zásobníka, pretečením rozsahu celých čísel a nesprávnou kontrolou pri načítavaní DLL knižníc. Tieto zraniteľnosti umožňujú vzdialenému útočníkovi spustiť škodlivý kód pomocou otvorenia infikovaného PDF súboru.
Jedna zo zraniteľností bola identifikovaná tímom CSIRT.SK a je evidovaná pod označením CVE-2016-1090.

Zraniteľné systémy:
Adobe Acrobat DC a Acrobat Reader DC Continuous verzie 15.010.20060 a nižšej
Adobe Acrobat DC a Acrobat Reader DC Classic verzie 15.006.30121 a nižšej
Adobe Acrobat XI a Reader XI verzie 11.0.15 a nižšej

Odporúčania:
Používateľom Windows odporúčame aktualizovať zraniteľný softvér na verzie 15.016.20039, resp. 15.006.30172, resp. 11.0.16. Aktualizáciu odporúčame vykonať čo najskôr.
Aktualizácie sú dostupné prostredníctvom stránky Adobe Acrobat Reader Download Center, prípadne prostredníctvom kontroly dostupných aktualizácii v uvedených produktoch.

Zdroje:
https://helpx.adobe.com/security/products/acrobat/apsb16-14.html

7-Zip

V programe 7-Zip boli nájdené a opravené dve kritické zraniteľnosti spôsobené čítaním mimo pridelenej pamäte a pretečením zásobníka. Tieto zraniteľnosti môžu viesť k spusteniu škodlivého kódu pri práci s UDF a HPS+ formátmi.

Zraniteľné systémy:
7-Zip verzie 15.14 a nižšej

Odporúčania:
Odporúčame aktualizovať program 7-Zip na najnovšiu verziu 16.02.

Zdroje:
http://blog.talosintel.com/2016/05/multiple-7-zip-vulnerabilities.html
http://www.7-zip.org/