

Mesačný prehľad kritických zraniteľností

Júl 2016

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2016-3204 skriptovacieho enginu VBScript a JScript je spôsobená chybami pri práci s objektmi v pamäti. Umožňuje vzdialené spustenie škodlivého kódu po navštívení infikovanej webovej stránky.

Zraniteľnosť CVE-2016-3238 Windows Print Spooler je spôsobená nedostatočnou kontrolou ovládača tlačiarne pred jeho inštaláciou. Útočník, ktorý kontroluje sieť (môže urobiť Man-in-the-Middle útok) alebo kontroluje tlačový server, môže túto zraniteľnosť zneužiť na vzdialené spustenie škodlivého kódu.

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 MS16-086, MS16-087 a taktiež aj MS16-093, 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 júlové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:

<https://technet.microsoft.com/en-us/library/security/ms16-086.aspx>

<https://technet.microsoft.com/en-us/library/security/ms16-087.aspx>

<https://technet.microsoft.com/en-us/library/security/ms16-093.aspx>

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosti CVE-2016-3278, CVE-2016-3280, CVE-2016-3281, CVE-2016-3282, CVE-2016-3283 a CVE-2016-3284 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).

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 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 MS16-088. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré uvedené zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si júlové Microsoft Security Bulletin dostupné na odkaze nižšie.

Zdroje:

<https://technet.microsoft.com/en-us/library/security/ms16-088.aspx>

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na 15 zraniteľností, z ktorých je 8 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 MS16-084. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si júlový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:

<https://technet.microsoft.com/en-us/library/security/ms16-084.aspx>

Microsoft Edge

Spoločnosť Microsoft vydala sadu záplat na 13 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.

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 júlový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:

<https://technet.microsoft.com/en-us/library/security/ms16-085.aspx>

Mozilla Firefox

Spoločnosť Mozilla nevydala v mesiaci júl žiadnu aktualizáciu prehliadača Firefox.

Zdroje:

<https://www.mozilla.org/sk/security/advisories/>

Google Chrome

Spoločnosť Google zverejnila jednu aktualizáciu prehliadača Chrome, ktorá obsahuje opravy 48 bezpečnostných zraniteľností.

Najväčšie zraniteľnosti umožňujú únik zo sandboxu pri použití PPAPI, spôsobiť pád aplikácie, XSS, url spoofing alebo iný, bližšie nešpecifikovaný dopad po načítaní infikovaných webstránok.

Zraniteľné systémy

Google Chrome do verzie 51.0.2704.106 a predchádzajúce

Odporúčania:

Odporúčame aktualizovať prehliadač na verziu 52.0.2743.82. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:

<http://googlechromereleases.blogspot.sk/2016/07/stable-channel-update.html>

4. Adobe Flash Player

Spoločnosť Adobe zverejnila jednu aktualizáciu opravujúcu 52 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), poškodením zásobníka a ďalšími chybami. Tieto zraniteľnosti umožňujú vzdialenému útočníkovi spustiť škodlivý kód alebo únik informácií pomocou infikovaného Flash obsahu.

Zraniteľné systémy:

Adobe Flash Player verzie 22.0.0.192 a nižšej

Adobe Flash Player verzie 18.0.0.360 a nižšej

Adobe Flash Player verzie 11.2.202.626 a nižšej

Odporúčania:

Používateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 22.0.0.209, používateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu 18.0.0.366. Používateľom Linux odporúčame aktualizovať na verziu 11.2.202.632.

Aktualizáciu odporúčame vykonať čo najskôr, nakoľko exploity na niektoré zraniteľnosti sú už používané.

Mesačný prehľad kritických zraniteľností

Aktualizácie sú dostupné prostredníctvom stránky Adobe Flash Player Download Center, prípadne prostredníctvom kontroly dostupných aktualizácií v produkte Adobe Flash Player.

Zdroje:

<https://helpx.adobe.com/security/products/flash-player/apsb16-25.html>

5. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft v mesiaci júl nevydala opravy žiadnych kritických zraniteľností platformy .NET. . Boli však zverejnené dôležité aktualizácie opravujúce zraniteľnosti spracovania XML dokumentov, ktoré umožňovali pri spracovávaní XML dokumentu prečítať ľubovoľný súbor na zariadení.

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 MS16-035. Odporúčame všetkým používateľom aktualizovať zraniteľný softvér. Správcom systémov odporúčame prezrieť si júlový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:

<https://technet.microsoft.com/en-us/library/security/ms16-091.aspx>

Oracle Java

Spoločnosť Oracle v mesiaci júl vydala bezpečnostnú aktualizáciu platformy Java opravujúcu 13 zraniteľností, z ktorých je 5 kritických.

Zraniteľnosti CVE-2016-3587, CVE-2016-3606, CVE-2016-3598, CVE-2016-3610 a CVE-2016-3552 umožňujú vzdialenému, resp. lokálnemu útočníkovi bez autentifikácie spustenie škodlivého kódu, kompromitáciu zariadenia, alebo iné bližšie neurčené dopady.

Zraniteľné systémy:

Java SE 6u115

Java SE 7u101

Java SE 8u92

Odporúčania:

Spoločnosť Oracle zverejnila aktualizáciu prostredníctvom bežného kanála Java Auto Update.

Mesačný prehľad kritických zraniteľností

Aktualizácie sú dostupné aj na stránke java.com. Používateľom odporúčame nainštalovať najnovšiu verziu Java SE 8 Update 101.

Zdroje:

<http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html>