Mesačný prehľad kritických zraniteľností
Apríl 2015

1. Operačné systémy Microsoft Windows

Kritická zraniteľnosť CVE-2015-1635 v ovládači HTTP.sys môže spôsobiť spustenie kódu na operačnom systéme Windows prostredníctvom zaslania špeciálne upraveného HTTP packetu. Útočník zmôže spustiť ľubovoľný kód s oprávneniami používateľa SYSTEM.

Zraniteľné systémy :
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 8 for 32-bit Systems
Windows 8 for x64-based Systems
Windows Server 2012
Windows Server 2012 R2
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2 (Server Core installation)

Zraniteľnosť CVE-2015-1645 spôsobená nesprávnym spracovaním metadát v obrázku vo formáte EMF môže spôsobiť vzdialené spustenie škodlivého kódu s právami prihláseného používateľa.

Zraniteľné systémy :
Windows Server 2003 Service Pack 2
Windows Server 2003 x64 Edition Service Pack 2
Windows Server 2003 with SP2 for Itanium-based Systems
Windows Vista Service Pack 2
Windows Vista x64 Edition Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for Itanium-based Systems Service Pack 2
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

Zraniteľnosť CVE-2015-0098 v komponente systému Windows Task Scheduler umožňuje eskalovať privilégia prihláseného používateľa na privilégia účtu SYSTEM v prípade možnosti plánovania úloh v systéme Windows.

Zraniteľné systémy :
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

Zraniteľnosti CVE-2015-1643 CVE-2015-1644 v systéme Windows umožňujú autentifikovanému používateľovi eskalovať privilégiá na úroveň administrátora. Chyby sú spôsobené nedostatočnou kontrolou oprávnení pri procese impersonácie akcií v systéme.

Zraniteľné systémy :
Windows Server 2003 R2 Service Pack 2
Windows Server 2003 Service Pack 2
Windows Server 2003 R2 x64 Edition Service Pack 2
Windows Server 2003 x64 Edition Service Pack 2
Microsoft Windows Server 2003 for Itanium-based Systems Service Pack 2
Windows Vista Service Pack 2
Windows Vista x64 Edition Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 8 for 32-bit Systems
Windows 8 for x64-based Systems
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
Windows Server 2012
Windows Server 2012 R2
Windows RT
Windows RT 8.1
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2012 (Server Core installation)

Windows Server 2012 R2 (server core installation)

Zraniteľnosť CVE-2015-1646 v komponente XML Core Services verzia 3 umožňuje po navštívení škodlivej URL linky obísť ochranu SAME origin policy a môže umožniť odcudzenie prihlasovacích cookies, hesiel a autentifikačných tokenov.

Zraniteľné systémy :
Windows Server 2003 Service Pack 2
Windows Server 2003 x64 Edition Service Pack 2
Windows Server 2003 with SP2 for Itanium-based Systems
Windows Vista Service Pack 2
Windows Vista x64 Edition Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for Itanium-based Systems Service Pack 2
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

Zraniteľnosť CVE-2015-1638 v Active Directory Federation services umožňuje únik informácií tak, že v prípade vypnutia prehliadača aplikácia, ktorá využíva na autentifikáciu AD FS nemusí odhlásiť používateľa a po opätovnom spustení prehliadača nežiada používateľa o autentifikáciu pred spustením aplikácie.

Zraniteľné systémy :
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 MS15-034, MS15-035, MS15-037 - MS15-041. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti už sú pravdepodobne používané. Správcom systémov odporúčame prezrieť si marcové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/library/security/MS15-034
https://technet.microsoft.com/en-us/library/security/ms15-035.aspx
https://technet.microsoft.com/en-us/library/security/ms15-037.aspx
https://technet.microsoft.com/en-us/library/security/ms15-038.aspx
https://technet.microsoft.com/en-us/library/security/ms15-039.aspx
https://technet.microsoft.com/en-us/library/security/ms15-040.aspx
https://technet.microsoft.com/en-us/library/security/ms15-041.aspx

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosť CVE-2015-1641 spôsobená poškodením pamäte umožňuje útočníkovi vzdialené spustenie škodlivého kódu s oprávneniami užívateľa, ktorý otvorí infikovaný súbor.

Zraniteľnosti CVE-2015-1650, CVE-2015-1649, CVE-2015-1651 spôsobené opätovným použitím uvoľnenej pamäte umožňuje útočníkovi vzdialené spustenie škodlivého kódu s oprávneniami užívateľa, ktorý otvorí infikovaný súbor.

Zraniteľné systémy:
Microsoft Word 2007 Service Pack 3
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Word 2010 Service Pack 2 (32-bit editions)
Microsoft Word 2010 Service Pack 2 (64-bit editions)
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 Service Pack 1 (64-bit editions)
Microsoft Word 2013 RT Service Pack 1
Microsoft Word Viewer
Microsoft Office Compatibility Pack Service Pack 3
Word Automation Services on Microsoft SharePoint Server 2010 Service Pack 2
Word Automation Services on Microsoft SharePoint Server 2013 Service Pack 1
Microsoft Office Web Apps Server 2010 Service Pack 2
Microsoft Office Web Apps Server 2013 Service Pack 1

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS15-033. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti už sú pravdepodobne používané.
Správcom systémov odporúčame prezrieť si marcový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms15-033.aspx

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na zraniteľnosti, ktoré sú spôsobené chybami pri práci s pamäťou a umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej stránky.
Jedná sa o zraniteľnosti CVE: CVE-2015-1652, CVE-2015-1657, CVE-2015-1659, CVE-2015-1660, CVE-2015-1662, CVE-2015-1665, CVE-2015-1666, CVE-2015-1667, CVE-2015-1668

Súčasne bola identifikovaná zraniteľnosť, ktorá umožňuje obchádzať ASLR v systéme Windows pod označením CVE-2015-1661.

Zraniteľné systémy:
Microsoft Internet Explorer 6 - 11

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS15-032. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko už boli zaznamenané exploity na niektoré zraniteľnosti. Správcom systémov odporúčame prezrieť si aprílové Microsoft Security Bulletin-y dostupné na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms15-032.aspx

Mozilla Firefox

Spoločnosť Mozilla vydala v mesiaci marec dve aktualizácie prehliadača Firefox opravujúce 3 zraniteľnosti, z toho 1 označená ako kritická.

Zraniteľnosť CVE-2015-0799 umožňuje potlačiť zobrazenie varovania o nesprávnom SSL certifikáte pri použití http/2 protokolu a Alt-Svc hlavičky, čo môže viesť k Man-in-the-Middle útoku, podstrčeniu falošného certifikátu a prístupu k zabezpečenej komunikácii.

Zraniteľné systémy:
Mozilla Firefox 36 a predchádzajúce
Mozilla Firefox ESR 31.5 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 37.0.1 a Mozilla Firefox ESR 31.6)
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 vydala šesť aktualizácií prehliadača Chrome, ktoré obsahujú opravy 54 bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť CVE-2015-1233 spôsobená chybou v interakcii medziprocesovej komunikácie, JavaScriptového enginu V8 a Gamepad API umožňuje vzdialenému útočníkovi spustiť škodlivý kód.

Ďalšie závažné zraniteľnosti sú najmä typu :

- Buffer Overflow : CVE-2015-1234
- User After Free : 2015-1237, CVE-2015-1245, CVE-2015-1243

Zraniteľné systémy
Google Chrome do verzie 42.0.2311.134

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 42.0.2311.134. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://googlechromereleases.blogspot.de/2015/04/stable-channel-update.html
http://googlechromereleases.blogspot.de/2015/04/stable-channel-update_14.html
http://googlechromereleases.blogspot.de/2015/04/stable-channel-update_28.html

4. Adobe Flash Player

Spoločnosť Adobe vydala v mesiaci apríl aktualizáciu opravujúcu 22 zraniteľností. Väčšina zraniteľnosti je spôsobená rôznymi chybami pri práci s pamäťou. Zraniteľnosti umožňujú vzdialenému útočníkovi spustenie škodlivého kódu, pričom niektoré boli použité pri reálnych útokoch (napríklad CVE-2015-3043)

CVE : CVE-2015-0346, CVE-2015-0347, CVE-2015-0348, CVE-2015-0349, CVE-2015-0350, CVE-2015-0351, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0356, CVE-2015-0357, CVE-2015-0358, CVE-2015-0359, CVE-2015-0360, CVE-2015-3038, CVE-2015-3039, CVE-2015-3040, CVE-2015-3041, CVE-2015-3042, CVE-2015-3043, CVE-2015-3044

Zraniteľné systémy

Adobe Flash Player 17.0.0.134 a nižšie
Adobe Flash Player 13.0.0.277 a nižšie
Adobe Flash Player 11.2.202.451 a nižšie
AIR Desktop Runtime 17.0.0.144 a nižšie
AIR SDK a SDK & Compiler 17.0.0.144 a nižšie

Odporúčania:

Užívateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 17.0.0.134, užívateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu 13.0.0.277. Užívateľom Linux odporúčame aktualizovať na verziu 11.2.202.451. Aktualizáciu odporúčame vykonať čo najskôr, nakoľko bolo zaznamenané použitie exploitov na niektoré zraniteľnosti.
Aktualizácie sú dostupné prostredníctvom stránky Adobe Flash Player Download Center, prípadne prostredníctvom kontroly dostupných aktualizácii v produkte Adobe Flash Player 16.x.

Zdroje:

https://helpx.adobe.com/security/products/flash-player/apsb15-06.html

5. Frameworky

Microsoft .NET Framework

Zraniteľnosť CVE-2015-1648 v ASP.NET umožňuje po zaslaní upraveného dotazu na webovú aplikáciu zobrazenie chyby v rámci ktorej môžu byť zobrazené aj citlivé údaje z konfiguračného súboru web.config (napríklad prihlasovacie údaje k databáze).

Zraniteľné systémy:
Microsoft .NET Framework 1.1 Service Pack 1,
Microsoft .NET Framework 2.0 Service Pack 2,
Microsoft .NET Framework 3.5,
Microsoft .NET Framework 3.5.1,
Microsoft .NET Framework 4,
Microsoft .NET Framework 4.5,
Microsoft .NET Framework 4.5.1,
Microsoft .NET Framework 4.5.2

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms15-041.aspx

Oracle Java

Spoločnosť Oracle v mesiaci apríl vydala bezpečnostnú aktualizáciu zahŕňajúcu 14 zraniteľností. Jedná sa o CVE: CVE-2015-0469, CVE-2015-0459, CVE-2015-0491, CVE-2015-0460, CVE-2015-0492, CVE-2015-0458, CVE-2015-0484, CVE-2015-0480, CVE-2015-0486, CVE-2015-0488, CVE-2015-0477, CVE-2015-0470, CVE-2015-0478, CVE-2015-0204. Z uvedených zraniteľností je 8 závažných umožňujúcich lokálnemu alebo vzdialenému neautentifikovanému používateľovi spustenie škodlivého kódu, prípadne kompromitáciu celého zariadenia. Niektoré z uvedených exploitov už boli použité pri reálnych útokoch.

Zdroje:
http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html

Odporúčania
Bezodkladná aktualizácia frameworku Java na aktuálnu podporovanú verziu.

V rámci vydaných bezpečnostných aktualizácií vydala spoločnosť Oracle bezpečnostné aktualizácie na databázový softvér MySQL. Odporúčame aktualizáciu na najnovšiu podporovanú verziu. V rámci aktualizácie bolo 34 zraniteľností v MySQL.