Mesačný prehľad kritických zraniteľností
Október 2014

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2014-4148 umožňuje vzdialené spustenie škodlivého kódu po otvorení infikovaného dokumentu alebo navštíveni infikovanej stránky obsahujúcej TrueType fonty. Zraniteľnosť CVE-2014-4113 vo Win32k.sys umožňuje prihlásenému útočníkovi eskaláciu práv, spúšťanie kódu v kernel móde, vytváranie administrátorských účtov.
Na obe zraniteľnosti boli objavené a použité exploity.

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 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 RT
Windows RT 8.1
Windows Server 2003 Service Pack 2
Windows Server 2003 x64 Edition Service Pack 2
Windows Server 2003 with SP2 for Itanium-based Systems
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 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 označením MS14-058. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti už sú známe a používané. Správcom systémov odporúčame prezrieť si októbrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:

http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=122
https://technet.microsoft.com/en-us/library/security/MS14-058

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosť CVE-2014-4117 umožňuje vzdialené spustenie škodlivého kódu po otvorení infikovaného dokumentu Microsoft Office Word.
Zraniteľnosti Windows OLE s označením CVE-2014-4114 umožňuje vzdialené spustenie škodlivého kódu po otvorení dokumentu Microsoft Office obsahujúceho infikovaný OLE objekt. Na túto zraniteľnosť bol objavený a použitý exploit.
Zraniteľnosti Windows OLE s označením CVE-2014-6352 umožňuje vzdialené spustenie škodlivého kódu po otvorení dokumentu Microsoft Office obsahujúceho infikovaný OLE objekt. Úspešné zneužitie zraniteľnosti vyžaduje interakciu užívateľa v podobe potvrdenia spustenia programu prostredníctvom dialogóveho okna UAC. Na túto zraniteľnosť je dostupný exploit v podobe infikovaného súboru Microsoft PowerPoint.

Zraniteľné systémy:

Microsoft Office 2007 Service Pack 3
Microsoft Office 2010 Service Pack 1 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office for Mac 2011
Microsoft Office Compatibility Pack Service Pack 3

Microsoft SharePoint Server 2010 Service Pack 1
Microsoft SharePoint Server 2010 Service Pack 2
Microsoft Office Web Apps 2010
Microsoft Office Web Apps 2010 Service Pack 1
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 MS14-060 a MS14-061. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti už sú známe a používané. Správcom systémov odporúčame prezrieť si októbrové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Na zraniteľnosť CVE-2014-6352 je dostupný workaround Microsoft Fix It na zabránenie možného zneužitia. Návod je dostupný na https://technet.microsoft.com/en-US/library/security/3010060#ID0EPG

Zdroje:

https://technet.microsoft.com/en-us/library/security/MS14-060
https://technet.microsoft.com/en-us/library/security/MS14-061

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na zraniteľnosti, z ktorých najzávažnejšie umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej stránky. Na zraniteľnosť CVE-2014-4123 už bol objavený a použitý exploit umožňujúci eskaláciu práv obídenim zabezpečenia IE Sandbox. Na mnohé ďalšie zraniteľnosti je výskyt exploitov a ich použitie pravdepodobné.

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 MS14-056. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti už sú známe a používané. Správcom systémov odporúčame prezrieť si októbrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/MS14-056

Mozilla Firefox

Spoločnosť Mozilla vydala novú verziu prehliadača Firefox opravujúcu nájdené zraniteľnosti, z ktorých sú tri označené ako kritické.
Zraniteľnosť CVE-2014-1578 umožňuje zápis mimo hraníc pri spracovávaní videa vo formáte WebM a následný pád aplikácie alebo možné spustenie škodlivého kódu.
Zraniteľnosti CVE-2014-1574 a CVE-2014-1575 spôsobené chybami pri práci s pamäťou umožňujúce pád aplikácie alebo možné spustenie škodlivého kódu.
Zraniteľnosť CVE-2014-1581 spôsobená opätovným využitím uvoľnenej pamäte pri interakcii so smerom textu umožňuje spustenie škodlivého kódu.

Zraniteľné systémy:
Mozilla Firefox 32 a predchádzajúce
Mozilla Firefox ESR 31.1 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé produkty na najnovšie verzie (Mozilla Firefox 33 a Mozilla Firefox 31.2).
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 a následne stiahnu aktualizácie.

Zdroje:
https://www.mozilla.org/security/advisories/mfsa2014-74/
https://www.mozilla.org/security/advisories/mfsa2014-77/
https://www.mozilla.org/security/advisories/mfsa2014-79/

Google Chrome

Spoločnosť Google vydala aktualizáciu prehliadača Chrome obsahujúcu 159 bezpečnostných opráv.
Najzávažnejšia zraniteľnosť CVE-2014-3138 spôsobená chybou v interakcii medzi IPC a Google V8 umožňuje vzdialeným útočníkom spustenie škodlivého kódu mimo sandboxu prehliadača pomocou vektora útoku využívajúceho JSON.

Zraniteľné systémy
Google Chrome do verzie 38.0.2125.101

Odporúčania:
Odporúčame aktualizovať prehliadač na najnovšiu verziu 38.0.2125.111. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=121
http://googlechromereleases.blogspot.in/2014/10/stable-channel-update.html

4. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft vydala dve sady záplat na zraniteľnosti .NET frameworku.
Najzávažnejšia zraniteľnosť CVE-2014-4121 umožňuje vzdialené spustenie škodlivého kódu vo webovej aplikácii .NET prostredníctvom infikovanej URI obsahujúcej medzinárnodné znaky.
XSS zraniteľnosť ASP.NET MVC frameworku s označením CVE-2014-4075 umožňuje obchádzanie bezpečnostných funkcií prostredníctvom kliknutia užívateľa na infikovaný odkaz alebo navštívením infikovanej webovej stránky.

Zraniteľné systémy:
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 4.5/4.5.1/4.5.2

ASP.NET MVC 2.0
ASP.NET MVC 3.0
ASP.NET MVC 4.0
ASP.NET MVC 5.0
ASP.NET MVC 5.1

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS14-057 a MS14-059. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti už sú známe a používané. Správcom systémov odporúčame prezrieť si októbrové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=122
https://technet.microsoft.com/en-us/library/security/MS14-057
https://technet.microsoft.com/en-us/library/security/MS14-059

Oracle Java

Spoločnosť Oracle vydala októbrovú sadu aktualizácií na zraniteľnosti Java SE. Najzávažnejšie zraniteľnosti komponentov AWT, Deployment, Libraries a Java FX s označeniami CVE-2014-6513, CVE-2014-6532, CVE-2014-6503, CVE-2014-6456, CVE-2014-6562 a CVE-2014-6485 umožňujú vzdialené spustenie škodlivého kódu a prevzatie kontroly nad operačným systémom obete.

Zraniteľné systémy:
Java SE 6u81
Java SE 7u67
Java SE 8u20
Java SE Embedded 7u60
JavaFX 2.2.65

Odporúčania:
Spoločnosť Oracle zverejnila aktualizáciu prostredníctvom bežného kanála Java Auto Update. Aktualizácie sú dostupné aj na stránke java.com. Používateľom odporúčame nainštalovať najnovšie verzie Java SE 8 Update 25, resp. Java SE 7 Update 71.

Zdroje:
http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html#AppendixJAVA
http://www.oracle.com/technetwork/topics/security/cpuoct2014verbose-1972962.html#JAVA

5. Iné závažné zraniteľnosti

Poodle útok na protokol SSL v3.0

Zraniteľnosť protokolu SSL v3.0 umožňujúca pomocou vhodného zarovnávania správ dešifrovať časť komunikácie a následne pri útoku typu MITM (Man in the middle) môže útočník vynútiť použitie staršieho protokolu SSL v3.0, aj keď obe strany podporujú novšie protokoly TLS. Zneužitím zraniteľnosti SSL v3.0 môže útočník dešifrovať časť komunikácie, získať cookies a previesť útoky typu session hijacking (ukradnúť identitu obete).

Zraniteľné systémy:
SSL v3.0

Odporúčania:
Odporúčame podporu SSL v3.0 vypnúť. Návody pre hlavné prehliadače aj možnosti otestovania zraniteľnosti systémov nájdete na http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=123.

Zdroje:
http://poodlebleed.com/
https://www.openssl.org/~bodo/ssl-poodle.pdf