Mesačný prehľad kritických zraniteľností
November 2014

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2014-6324 v implementácii Kerberos KDC (Key Distribution Center) spôsobená nesprávnou kontrolou podpisov ticketov. Za určitých okolností tak môže neprivilegovaný užívateľ v doméne vytvoriť falošný ticket, pomocou ktorého získa administrátorské oprávnenia.
Zraniteľnosť CVE-2014-6321 Microsoft Secure Channel (Schannel). Schannel je Microsoft implementácia protokolov SSL a TLS. Zraniteľnosť je spôsobená nesprávnym spracovaním nekorektných packetov. Vzdialený útočník môže pomocou odoslania nekorektného packetu vynútiť spustenie škodlivého kódu na cieľovom zariadení a kompromitovať tak napadnutý systém.
Zraniteľnosť CVE-2014-6332 Microsoft Windows OLE spôsobená nesprávnou kontrolou pri zmene veľkosti poľa. To umožňuje vzdialenému útočníkovi vytvoriť škodlivú stránku, ktorá po zobrazení v Internet Exploreri modifikuje pamäť. Následne sa spustí škodlivý kód, ktorý dokáže obísť sandbox Internet Explorera aj zabezpečenie EMET (Enhanced Mitigation Experience Toolkit).
Zraniteľnosť CVE-2014-4118 Microsoft XML Core Services (MSXML) spôsobená nesprávnym spracovaním XML dokumentov. Umožňuje vzdialenému útočníkovi spustenie škodlivého kódu po otvorení infikovanej webstránky alebo dokumentu.

Na uvedené zraniteľnosti (okrem poslednej) už 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 označeniami MS14-064, MS14-066, MS14-067 a MS14-068. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti už sú verejne dostupné a používané. Správcom systémov odporúčame prezrieť si novembrové Microsoft Security Bulletin dostupný na odkazoch nižšie.

Zdroj:
https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=124
https://technet.microsoft.com/library/security/MS14-064
https://technet.microsoft.com/library/security/MS14-066
https://technet.microsoft.com/library/security/MS14-067
https://technet.microsoft.com/library/security/MS14-068

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosti CVE-2014-6333, CVE-2014-6334 a CVE-2014-6335 spôsobené chybami pri práci s objektmi v pamäti pri spracovaní nekorektnýchdokumentov. Zraniteľnosti umožňujú vzdialené spustenie škodlivého kódu po otvorení infikovaného dokumentu Microsoft Office.

Zraniteľné systémy:
Microsoft Office 2007 Service Pack 3
Microsoft Word Viewer
Microsoft Office Compatibility Pack Service Pack 3

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS14-069. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti už sú pravdepodobne používané.
Správcom systémov odporúčame prezrieť si novembrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/library/security/MS14-069

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 Internet Explorera prostredníctvom Windows OLE s označením CVE-2014-6332 je verejne známy exploit v podobe modulu do Metasploitu umožňujúci vzdialené spustenie škodlivého kódu a obchádza IE Sandbox aj zabezpečenie EMET. 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 MS14-065. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti už sú známe a používané. Správcom systémov odporúčame prezrieť si novembrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=124
https://technet.microsoft.com/library/security/MS14-065

Mozilla Firefox

Spoločnosť Mozilla vydala minoritnú aktualizáciu prehliadača Firefox, zameriavajúcu sa na lepšiu ochranu súkromia. Neboli zverejnené žiadne opravy kritických zraniteľností.

Odporúčania:
Užívateľom, ktorí by chceli využívať vyhľadávač DuckDuckGo alebo zjednodušené vymazanie histórie, odporúčame aktualizovať prehliadač na najnovšiu verziu Mozilla Firefox 33.1.1. 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/en-US/firefox/33.1/releasenotes/
https://www.mozilla.org/en-US/firefox/33.1.1/releasenotes/

Google Chrome

Spoločnosť Google vydala tri aktualizácie prehliadača Chrome, z ktorých najväčšia obsahuje 42 bezpečnostných opráv.
Najzávažnejšia zraniteľnosť CVE-2014-0574 spôsobená opätovným uvoľnením predtým uvoľnenej pamäte v Adobe Flash Player umožňuje vzdialeným útočníkom spustenie škodlivého kódu. Ďalšie vážne zraniteľnosti umožňujú útoky typu zamietnutie služby.

Zraniteľné systémy
Google Chrome do verzie 39.0.2171.71

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 39.0.2171.71. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://googlechromereleases.blogspot.in/2014/11/stable-channel-update.html
http://googlechromereleases.blogspot.in/2014/11/stable-channel-update_18.html
http://googlechromereleases.blogspot.in/2014/11/stable-channel-update_25.html

4. Adobe Flash Player

Spoločnosť Adobe vydala v mesiaci november dve aktualizácie opravujúce 19 zraniteľností. Zraniteľnosti sú spôsobené rôznymi chybami pri práci s pamäťou a umožňujú vzdialenému útočníkovi spustenie škodlivého kódu, eskaláciu privilégií a odhalenie citlivých informácií (session tokeny). Opravená je aj kritická zraniteľnosť CVE-2014-8439, ktorá bola zmiernená októbrovými aktualizáciami, avšak medzičasom už boli zaznamenané exploity,ktoré dokázali obísť októbrovú záplatu.

Zraniteľné systémy
Adobe Flash Player do verzie 15.0.0.223
Adobe Flash Player do verzie 13.0.0.252
Adobe Flash Player do verzie 11.2.202.418

Odporúčania:
Užívateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 15.0.0.239, užívateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu 13.0.0.258. Užívateľom Linux odporúčame aktualizovať na verziu 11.2.202.424. Aktualizáciu odporúčame vykonať čo najskôr, nakoľko boli zaznamenané exploity na niektoré zraniteľnosti.
Aktualizácie sú dostupné prostredníctvom stránky Adobe Flash Player Download Center, prípadne prostredníctvom kontroly dostupných aktualizácii v produkte Adobe Flash Player 15.x.

Zdroje:
http://helpx.adobe.com/security/products/flash-player/apsb14-24.html
http://helpx.adobe.com/security/products/flash-player/apsb14-26.html

5. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft vydala záplatu na zraniteľnosť .NET frameworku spôsobenú nesprávnou kontrolou TypeFilterLevel. Zraniteľnosť útočníkovi umožňuje eskaláciu práv a vzdialené spustenie škodlivého kódu odoslaním infikovaných dát klientskej stanici alebo serveru využívajúcemu .NET Remoting.

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 4.5/4.5.1/4.5.2

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplata na uvedenú zraniteľnosť je distribuovaná pod označením MS14-072. Odporúčame všetkým používateľom čo aktualizovať zraniteľný softvér. Správcom systémov odporúčame prezrieť si novembrové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/library/security/MS14-072

Oracle Java

Spoločnosť Oracle nevydala v mesiaci žiadnu aktualizáciu platformy Java. Najbližšia veľká sada aktualizácii je naplánovaná na 20. január 2015.

Zdroje:
http://www.oracle.com/technetwork/topics/security/alerts-086861.html

6. Iné závažné zraniteľnosti

Špionážny nástroj Regin

Spoločnosť Symantec zverejnila analýzu o novom pokročilom špionážnom nástroji Regin. Regin je modulárny viacúrovňový Trójsky kôň so vzdialeným prístupom (RAT), ktorý môže obsahovať rôzne komponenty v závislosti od konkrétneho typu útoku a útočníkom umožňuje

veľmi špecifické zameranie sa na individuálne ciele. Nástroj Regin je určený hlavne na dlhodobé sledovanie a zbieranie dát spoločností aj jednotlivcov. Medzi jeho schopnosti patrí napríklad kontrolovanie vstupných zariadení (odchytávanie klávesnice, myši), vytváranie snímok obrazovky, kradnutie prihlasovacích údajov, monitorovanie sieťovej prevádzky, zbieranie informácii o využití systému (sledovanie procesov, vyťaženia pamäte,...).

Odporúčania:
Používateľom aj administrátorom odporúčame používať antivírusové riešenie a pravidelne aktualizovať antivírusovú databázu, nakoľko prevažná väčšina antivírov už v súčasnosti deteguje prítomnosť niektorých komponentov nástroja Regin.
Administrátorom ďalej odporúčame udržiavať operačný systém aj nainštalované aplikácie aktuálne a nepodceňovať dôležitosť bezpečnostných záplat.

Zdroje:
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf
https://www.us-cert.gov/ncas/alerts/TA14-329A

Verejne dostupné IP kamery

Server insecam.org zverejnil zoznam nezabezpečených, resp. zle zabezpečených kamier dostupných prostredníctvom Internetu. Uvedené kamery používajú prednastavené prihlasovacie údaje a ktokoľvek sa tak na ne môže pripojiť a sledovať ich obraz. Stránka obsahovala aj desiatky kamier zo Slovenska, avšak v čase písania tejto správy už nie sú dostupné žiadne kamery zo Slovenska.

Odporúčania:
Prevádzkovateľom kamier pripojených na Internet odporúčame skontrolovať ich zabezpečenie a zmeniť prednastavené heslá.

Zdroje:
http://www.insecam.org/