Mesačný prehľad kritických zraniteľností
Január 2016

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2016-0002 skriptovacieho enginu VBScript je spôsobená chybami pri práci s objektmi v pamäti. Umožňuje vzdialené spustenie škodlivého kódu po navštívení infikovanej webovej stránky.

Zraniteľnosť CVE-2016-0008 vo Windows Kernel Mode Drivers v komponente Graphics Device Interface (GDI) je spôsobená chybami pri práci s objektmi v pamäti. Útočníkovi umožňuje obísť bezpečnostnú ochranu Address Space Layout Randomization (ASLR).

Zraniteľnosť CVE-2016-0009 vo Windows Kernel Mode Drivers v komponente Win32k je spôsobená chybami pri práci s objektmi v pamäti. Umožňuje vzdialené spustenie škodlivého kódu po navštívení infikovanej webovej stránky.

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 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
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 MS16-003 a MS16-005. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko niektoré zraniteľnosti boli publikované verejne a použitie exploitov na uvedené zraniteľnosti je pravdepodobné.
Správcom systémov odporúčame prezrieť si januárové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-003.aspx
https://technet.microsoft.com/en-us/library/security/ms16-005.aspx

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosti CVE-2016-0010 a CVE-2016-0035 sú spôsobené chybami pri práci s pamäťou. Útočníkovi umožňujú vzdialené spustenie škodlivého kódu po otvorení infikovaných súborov Microsoft Office.

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 editions)
Microsoft Office 2016 (64-bit editions)

Microsoft Office for Mac 2011
Microsoft Office for Mac 2016
Microsoft Excel Viewer
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 MS16-004. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko niektoré zraniteľnosti boli publikované verejne a použitie exploitov na uvedené zraniteľnosti je pravdepodobné.
Správcom systémov odporúčame prezrieť si januárový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-004.aspx

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala jednu sadu záplat na 2 zraniteľnosti, z ktorých je 1 označená ako kritická. Zraniteľnosť CVE-2016-0002 je spôsobená chybami pri práci s pamäťou v skriptovacom engine VBScript a umožňuje vzdialené spustenie škodlivého kódu po navštívení infikovanej stránky.

Zraniteľné systémy:
Microsoft Internet Explorer 7
Microsoft Internet Explorer 8
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 MS16-001. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedené zraniteľnosti je pravdepodobný. Správcom systémov odporúčame prezrieť si januárové Microsoft Security Bulletin dostupné na odkaze nižšie.

Upozornenie:
Pokiaľ používate na jednotlivých systémoch staršie verzie prehliadača Internet Explorer, odporúčame čo najskôr aktualizovať na najnovšiu dostupnú verziu pre daný operačný systém, pretože od 12. januára 2016 staršie verzie prehliadača nebudú podporované a nebudú dostávať bezpečnostné záplaty. Ďalej budú podporované už iba najnovšie verzie tohto prehliadača pre jednotlivé podporované operačné systémy. Zhrnutie podporovaných verzií Internet Exploreru pre desktopové systémy uvádzame v nasledujúcej tabuľke:

Windows Vista Service Pack 2	Internet Explorer 9
Windows 7 Service Pack 1	Internet Explorer 11
Windows 8	Internet Explorer 11
Windows 8.1	Internet Explorer 11

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-001.aspx
https://www.microsoft.com/en-us/WindowsForBusiness/End-of-IE-support

Microsoft Edge

Spoločnosť Microsoft vydala jednu sadu záplat na 2 zraniteľnosti, z ktorých sú obe 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 MS16-002. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedené zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si decembrové Microsoft Security Bulletin dostupné na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-002.aspx

Mozilla Firefox

Spoločnosť Mozilla vydala v mesiaci september jednu aktualizáciu prehliadača Firefox opravujúce 4 kritické zraniteľnosti.

Zraniteľnosť CVE-2016-1946 v knižnici libstagefright umožňuje zápis za hranicami buffera, čo môže byť zneužité na vzdialené spustenie škodlivého kódu po zobrazení infikovaného videa vo formáte MP4.

Zraniteľnosť CVE-2016-1935 vo WebGL môže byť zneužitá na vzdialené spustenie škodlivého kódu po zobrazení infikovaného WebGL obsahu.

Zraniteľnosti CVE-2016-1930 a CVE-2016-1931 spôsobené bližšie nešpecifikovanými chybami pri práci s pamäťou môžu viesť k vzdialenému spusteniu škodlivého kódu.

Zraniteľné systémy:
Mozilla Firefox 43.0.4 a predchádzajúce
Mozilla Firefox ESR 38.5 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 44.0 a Mozilla Firefox ESR 38.6)
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 zverejnila tri aktualizácie prehliadača Chrome, ktoré obsahujú opravy 38 bezpečnostných zraniteľností.

Najvážnejšie zraniteľnosti umožňujú spôsobiť pád aplikácie alebo iný, bližšie nešpecifikovaný dopad po načítaní infikovaných webstránok alebo PDF súborov.

Zraniteľné systémy
Google Chrome do verzie 47.0.2526.111 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 48.0.2564.82, prípadne 48.0.2564.97. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://googlechromereleases.blogspot.in/2016/01/stable-channel-update.html
http://googlechromereleases.blogspot.in/2016/01/stable-channel-update_20.html
http://googlechromereleases.blogspot.in/2016/01/stable-channel-update_27.html

4. Adobe Flash Player

Spoločnosť Oracle v mesiaci január nevydala žiadne aktualizácie prehrávača Adobe Flash Player.

Zdroje:
https://helpx.adobe.com/security.html

5. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft v mesiaci január nevydala žiadne aktualizácie platformy Microsoft .NET Framework.

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

Oracle Java

Spoločnosť Oracle v mesiaci január vydala bezpečnostnú aktualizáciu platformy Java obsahujúcu 8 zraniteľností, z ktorých sú 3 kritické.

Zraniteľnosti CVE-2016-0494, CVE-2015-8126 a CVE-2016-0483 umožňujú vzdialenému útočníkovi bez autentifikácie spustenie škodlivého kódu, prípadne kompromitáciu zariadenia.

Zraniteľné systémy:
Java SE 6u105
Java SE 7u91
Java SE 8u66

Odporúčania:
Spoločnosť Oracle zverejnila aktualizáciu prostredníctvom bežného kanála Java Auto Update. Aktualizácie sú dostupné aj na stránke java.com. Používateľom odporúčame nainštalovať najnovšiu verziu Java SE 8 Update 71.

Zdroje:
http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html

6. Iné závažné zraniteľnosti

Eskalácia práv v Linuxe

Zraniteľnosť CVE-2016-0728 v Linuxovom jadre spôsobená nesprávnym počítaním referencií na objekt kľúčenky (keyring). Táto chyba môže viesť k pretečeniu počítadla referencií a uvoľneniu pamäte alokovanej pre objekt kľúčenky. Útočník môže následne vynútiť znovupoužitie tejto pamäte (use-after-free) a dosiahnuť tak spustenie vlastného kódu s právami superpoužívateľa. Zraniteľné boli systémy s Linuxovým jadrom verzie 3.8 a novšej. Momentálne už je chyba opravená, pričom zmiernenie rizika jej zneužitia je možné dosiahnuť pomocou ochranných mechanizmov ako ASLR, SMEP, SMAP, ktoré sú zvyčajne v prednastavenej konfigurácii zapnuté.

Zdroje:
http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=143
http://perception-point.io/2016/01/14/analysis-and-exploitation-of-a-linux-kernel-vulnerability-cve-2016-0728/