Mesačný prehľad kritických zraniteľností December 2015

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2015-6136 skriptovacieho enginu VBScript je spôsobená chybami pri práci s objektmi v pamäti. Umožňuje vzdialené spustenie škodlivého kódu po navštívení infikovanej webovej stránky.

Zraniteľnosť CVE-2015-6125 serverov Windows DNS je spôsobená znovupoužitím uvošnenej pamäti pri spracovaní DNS požiadaviek. Útočníkovi umožňuje po odoslaní škodlivej DNS požiadavky serveru vykonať vzdialené spustenie škodlivého kódu so systémovými oprávneniami.

Zraniteľnosti CVE-2015-6106, CVE-2015-6107 a CVE-2015-6108 sú spôsobené chybami pri spracovaní vložených fontov v dokumentoch. Umožňujú vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení dokumentu obsahujúceho infikované vložené fonty. Útočník zneužitím tejto zraniteľnosti môže získať systémové práva a prevziať kontrolu nad zariadením.

Zraniteľnosť CVE-2015-6130 vo Windows Uniscribe (API pre renderovanie komplexného Unicode textu) je spôsobená chybami pri práci s celými číslami typu Integer Underflow pri spracovaní infikovaných fontov. Umožňujú vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení dokumentu obsahujúceho infikované vložené fonty. Útočník zneužitím tejto zraniteľnosti môže získať systémové práva a prevziať kontrolu nad zariadením.

Zraniteľnosti CVE-2015-6171, CVE-2015-6173, CVE-2015-6174 a CVE-2015-6175 vo Windows Kernel-Mode Drivers sú spôsobené chybami pri práci s objektmi v pamäti. Prihlásenému útočníkovi umožňujú po spustení škodlivého kódu získať oprávnenia na úrovni systému a prevziať kontrol nad zariadením. Zraniteľnosť CVE-2015-6175 je aktívne zneužívaná útočníkmi.

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 MS15-126, MS15-127, MS15-128, MS15-130 a MS15-135. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko bolo zaznamenané použitie exploitov na niektoré zraniteľnosti a použitie exploitov na ostatné uvedené zraniteľnosti je pravdepodobné.
Správcom systémov odporúčame prezrieť si decembrové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms15-126.aspx
https://technet.microsoft.com/en-us/library/security/ms15-127.aspx
https://technet.microsoft.com/en-us/library/security/ms15-128.aspx
https://technet.microsoft.com/en-us/library/security/ms15-130.aspx
https://technet.microsoft.com/en-us/library/security/ms15-135.aspx

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosť CVE-2015-6172 v Microsoft Outlook pri spracovávaní emailov. Zobrazenie infikovaného emailu môže byť zneužité na vzdialené spustenie škodlivého kódu.

Zraniteľnosti CVE-2015-6040, CVE-2015-6118, CVE-2015-6122, CVE-2015-6124 a CVE-2015-6177 sú spôsobené chybami pri práci s pamäťou a umožňujú útočníkovi vzdialené spustenie škodlivého kódu po otvorení infikovaných súborov Microsoft Office. Bolo zaznamenané použitie exploitov na zraniteľnosť CVE-2015-6124.

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 MS15-131. Odporúčame všetkým používateľom čo aktualizovať zraniteľný softvér, nakoľko bolo zaznamenané použitie exploitov na zraniteľnosť CVE-2015-6124 a použitie exploitov na ostatné uvedené zraniteľnosti je pravdepodobné.
Správcom systémov odporúčame prezrieť si decembrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms15-131.aspx

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala jednu sadu záplat na 30 zraniteľnosti, z ktorých je 23 označených ako kritických, sú spôsobené chybami pri práci s pamäťou v prehliadači a skriptovacích enginoch VBScript a umožňujú 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 MS15-112. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré 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/ms15-124.aspx

Microsoft Edge

Spoločnosť Microsoft vydala jednu sadu záplat na 15 zraniteľnosti, z ktorých je 10 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 MS15-113. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré 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/ms15-125.aspx

Mozilla Firefox

Spoločnosť Mozilla vydala v mesiaci september jednu aktualizáciu prehliadača Firefox opravujúce 5 kritických zraniteľností.

Zraniteľnosť CVE-2015-7210 vo WebRTC spôsobená nesprávnym časovaním počas zatvárania dátových kanálov umožňuje vzdialené spustenie škodlivého kódu.

Zraniteľnosť CVE-2015-7214 umožňuje obísť zabezpečenie Same-origin-policy pomocou view-source: a data: URI.

Zraniteľnosť CVE-2015-7223 vo WebExtension API môže byť zneužitá na spustenie kódu s oprávnením rozšírenia prehliadača používajúceho volania týchto API funkcií.

Zraniteľnosti CVE-2015-7201 a CVE-2015-7202 spôsobené bližšie nešpecifikovanými chybami pri práci s pamäťou môžu viesť k vzdialenému spusteniu škodlivého kódu.

Zraniteľné systémy:
Mozilla Firefox 42.0 a predchádzajúce
Mozilla Firefox ESR 38.4 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 43.0.2 a Mozilla Firefox ESR 38.5)
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 50 bezpečnostných zraniteľností aj novú verziu Adobe Flash Player.

Zraniteľnosť CVE-2015-6765 je spôsobená znovupoužitím uvoľnenej pamäte pri práci s AppCache a umožňuje vzdialené spustenie škodlivého kódu.

Ďalšie vážne zraniteľnosti umožňujú spôsobiť pád aplikácie, obísť zabezpečenie Same-origin-policy alebo iný, bližšie nešpecifikovaný dopad po načítaní infikovaných webstránok alebo PDF súborov.

Zraniteľné systémy
Google Chrome do verzie 47.0.2526.80 (vrátane)

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 47.0.2526.106. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://googlechromereleases.blogspot.in/2015/12/stable-channel-update.html
http://googlechromereleases.blogspot.in/2015/12/stable-channel-update_8.html
http://googlechromereleases.blogspot.in/2015/12/stable-channel-update_15.html

4. Adobe Flash Player

Spoločnosť Adobe zverejnila dve aktualizácie opravujúce 98 zraniteľnosti, všetky sú označené ako kritické.

Zraniteľnosti sú spôsobené opätovným použitím uvoľnenej pamäte, použitím nesprávnych typov premenných, pretečením pamäte, pretečením rozsahu celých čísel a ďalšími chybami. Tieto zraniteľnosti umožňujú vzdialenému útočníkovi spustiť škodlivý kód pomocou infikovaného Flash obsahu.
Bolo zaznamenané aktívne zneužívanie zraniteľnosti CVE-2015-8651 v cielených útokoch.

Zraniteľné systémy
Adobe Flash Player verzie 20.0.0.235 a nižšej
Adobe Flash Player verzie 18.0.0.268 a nižšej
Adobe Flash Player verzie 11.2.202.554 a nižšej

Odporúčania:
Používateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 20.0.0.267, používateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu 18.0.0.324. Používateľom Linux odporúčame aktualizovať na verziu 11.2.202.559.

Aktualizáciu odporúčame vykonať čo najskôr, nakoľko exploity na niektoré zraniteľnosti sú už používané.
Aktualizácie sú dostupné prostredníctvom stránky Adobe Flash Player Download Center, prípadne prostredníctvom kontroly dostupných aktualizácii v produkte Adobe Flash Player.

Zdroje:
https://helpx.adobe.com/security/products/flash-player/apsb15-32.html
https://helpx.adobe.com/security/products/flash-player/apsb16-01.html

5. Frameworky

Microsoft .NET Framework

Zraniteľnosť CVE-2015-6108 je spôsobená chybou pri spracovaní vložených fontov v dokumentoch. Umožňuje vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení dokumentu obsahujúceho infikované vložené fonty. Útočník zneužitím tejto zraniteľnosti môže získať systémové práva a prevziať kontrolu nad zariadením.

Zraniteľné systémy
Microsoft .NET Framework 3.0 Service Pack 2
Microsoft .NET Framework 3.5/3.5.1
Microsoft .NET Framework 4
Microsoft .NET Framework 4.5/4.5.1/4.5.2
Microsoft .NET Framework 4.6

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS15-128. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedenú zraniteľnosť je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si decembrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms15-128.aspx

Oracle Java

Spoločnosť Oracle v mesiaci december nevydala žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 19. január 2016.

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