

Mesačný prehľad kritických zraniteľností

November 2015

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2015-6097 aplikácie Windows Denník (Journal) spôsobená chybou pri spracovaní súborov Windows Denník (.jnt) môže spôsobiť pretečenie pamäti na halde a následné vzdialené spustenie škodlivého kódu po otvorení infikovaného súboru Windows Denník.

Zraniteľnosti CVE-2015-6103 a CVE-2015-6104 v knižnici Adobe Type Manager sú spôsobené chybami pri spracovaní fontov vložených 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.

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. Zápłaty na uvedené zraniteľnosti sú distribuované pod označeniami

Mesačný prehľad kritických zraniteľností

MS15-114 a MS15-115. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko použitie exploitov na uvedené zraniteľnosti je pravdepodobné. Správcom systémov odporúčame prezrieť si novembrové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:

<https://technet.microsoft.com/en-us/library/security/ms15-114.aspx>

<https://technet.microsoft.com/en-us/library/security/ms15-115.aspx>

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft v mesiaci november nevydala opravy žiadnych kritických zraniteľností kancelárskych balíkov Microsoft Office a Office Web Apps. Boli však zverejnené dôležité aktualizácie opravujúce zraniteľnosti spôsobené chybami pri práci s pamäťou umožňujúce vzdialené spustenie škodlivého kódu po otvorení infikovaného súboru.

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

Microsoft SharePoint Server 2007 Service Pack 3 (32-bit editions)
Microsoft SharePoint Server 2007 Service Pack 3 (64-bit editions)
Microsoft SharePoint Server 2010 Service Pack 2
Microsoft SharePoint Server 2013 Service Pack 1

Microsoft Office Web Apps 2010 Service Pack 2
Microsoft Office Web Apps 2013 Service Pack 1

Odporúčania:

Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS15-116. Odporúčame všetkým používateľom čo aktualizovať zraniteľný softvér, nakoľko použitie exploitov na uvedené zraniteľnosti je pravdepodobné.

Správcom systémov odporúčame prezrieť si novembrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:

<https://technet.microsoft.com/en-us/library/security/ms15-116.aspx>

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala jednu sadu záplat na 25 zraniteľnosti, z ktorých je 23 označených ako kritických, sú spôsobené chybami pri práci s pamäťou v prehliadači a skriptovacích enginoch VBScript a JScript 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 novembrové Microsoft Security Bulletin dostupné na odkaze nižšie.

Zdroj:

<https://technet.microsoft.com/en-us/library/security/ms15-112.aspx>

Microsoft Edge

Spoločnosť Microsoft vydala jednu sadu záplat na 4 zraniteľnosti, z ktorých sú 2 označené ako kritické, sú spôsobené chybami pri práci s pamäťou a 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. Správcom systémov odporúčame prezrieť si novembrové Microsoft Security Bulletin dostupné na odkaze nižšie.

Zdroj:

<https://technet.microsoft.com/en-us/library/security/ms15-113.aspx>

Mozilla Firefox

Spoločnosť Mozilla vydala v mesiaci september jednu aktualizáciu prehliadača Firefox opravujúce 8 kritických zraniteľností.

Zraniteľnosti CVE-2015-7181, CVE-2015-7182 a CVE-7183 v Mozilla Network Security Services (NSS) a Netscape Portable Runtime (NSPR) sú spôsobené opätovným použitím uvonenej pamäte, pretečením pamäte (buffer overflow) a pretečením celočíselných premenných. Zraniteľnosti umožňujú vzdialené spustenie škodlivého kódu.

Zraniteľnosť CVE-2015-7198 v grafickej knižnici ANGLE je spôsobená pretečením pamäte (buffer overflow) a umožňuje spôsobiť pád aplikácie pri spracovaní textúr.

Zraniteľnosť CVE-2015-7199 spôsobená chýbajúcou kontrolou stavu umožňuje spôsobiť pád aplikácie pri spracovaní SVG obrázkov.

Zraniteľnosť CVE-2015-7200 spôsobená chýbajúcou kontrolou stavu v implementácii rozhrania CryptoKey môže mať bližšie nešpecifikovaný dopad pri spracovaní kryptografických kľúčov.

Zraniteľnosti CVE-2015-4513 a CVE-2015-4514 spôsobené bližšie nešpecifikovanými chybami pri práci s pamäťou môžu viesť k vzdialenému spusteniu škodlivého kódu.

Zraniteľné systémy:

Mozilla Firefox 41.0.2 a predchádzajúce

Mozilla Firefox ESR 38.3 a predchádzajúce

Odporúčania:

Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 42 a Mozilla Firefox ESR 38.4)

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 jednu aktualizáciu prehliadača Chrome, ktorá obsahuje opravy bezpečnostných zraniteľností aj novú verziu Adobe Flash Player.

Mesačný prehľad kritických zraniteľností

Najväčšia opravená zraniteľnosť CVE-2015-1302 umožňuje obísť zabezpečenie Same-origin-policy prostredníctvom integrovaného PDF prehliadača.

Zraniteľné systémy

Google Chrome do verzie 46.0.2490.80 (vrátane)

Odporúčania:

Odporúčame aktualizovať prehliadač na verziu 46.0.2490.86. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:

<http://googlechromereleases.blogspot.in/2015/11/stable-channel-update.html>

4. Adobe Flash Player

Spoločnosť Adobe zverejnila aktualizáciu opravujúcu 17 zraniteľností, všetky sú označené ako kritické.

Zraniteľnosti sú spôsobené opätovným použitím uvoľnenej pamäte, použitím nesprávnych typov premenných a ďalšími chybami. Tieto zraniteľnosti umožňujú vzdialenému útočníkovi spustiť škodlivý kód pomocou infikovaného Flash obsahu alebo vytvárať súbory v súborovom systéme s prístupovými právami užívateľa.

Zraniteľné systémy

Adobe Flash Player verzie 19.0.0.226 a nižšej

Adobe Flash Player verzie 18.0.0.255 a nižšej

Adobe Flash Player verzie 11.2.202.540 a nižšej

Odporúčania:

Používateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 19.0.0.245, používateľom Adobe Flash Player s predĺženou podporou odporúčame aktualizovať na verziu 18.0.0.261. Používateľom Linux odporúčame aktualizovať na verziu 11.2.202.548.

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 aktualizácií v produkte Adobe Flash Player.

Zdroje:

<https://helpx.adobe.com/security/products/flash-player/apsb15-28.html>

5. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft v mesiaci november nevydala opravy žiadnych kritických zraniteľností platformy .NET. Boli však zverejnené dôležité aktualizácie opravujúce zraniteľnosti umožňujúce prečítanie lokálnych súborov na počítači, vloženie skriptu do prehliadača obete,

Mesačný prehľad kritických zraniteľností

prípadne obídanie ochrany ASLR po otvorení infikovaného súboru alebo navštívení infikovanej webstránky.

Zraniteľné systémy

Microsoft .NET Framework 2.0 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 MS15-118. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré zraniteľnosti je vysoko pravdepodobný. Správcov systémov odporúčame prezrieť si novembrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:

<https://technet.microsoft.com/en-us/library/security/ms15-118.aspx>

Oracle Java

Spoločnosť Oracle v mesiaci november 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>