Mesačný prehľad kritických zraniteľností
November 2016

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2016-7212 je spôsobená chybami pri načítavaní obrázkov. Umožňuje vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení emailu obsahujúceho infikovaný obrázok.

Zraniteľnosť CVE-2016-7248 v komponente Microsoft Video Control je spôsobená chybami pri práci s objektmi v pamäti. Umožňuje vzdialené spustenie škodlivého kódu po otvorení infikovaného súboru alebo aplikácie z webstránky alebo emailu.

Zraniteľnosť CVE-2016-7205 vo Windows Animation Manager je spôsobená chybami pri práci s objektmi v pamäti. Umožňuje vzdialené spustenie škodlivého kódu po navštívení webstránky. Útočník môže zneužitím tejto zraniteľnosti prevziať kontrolu nad zariadením.

Zraniteľnosť CVE-2016-7256 vo Windows Font Library je spôsobená chybami pri práci s Open Type fontami. Umožňuje vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení infikovaného dokumentu. Útočník môže zneužitím tejto zraniteľnosti prevziať kontrolu nad zariadením. Bolo zaznamenané zneužitie tejto zraniteľnosti útočníkmi.

Zároveň bola opravená zraniteľnosť CVE-2016-7255 publikovaná spoločnosťou Google, o ktorej sme uvádzali ako neopravenú v októbrovom mesačníku. Zraniteľnosť v komponente Win32k je spôsobená chybami pri práci s objektmi v pamäti. Umožňuje zvýšenie privilégií po spustení infikovaného programu a bolo zaznamenané aktívne zneužívanie 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 8.1 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 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
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)
Windows Server 2016 for x64-based Systems

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označeniami MS16-130, MS16-131, MS16-132, MS16-135 a taktiež aj MS16-141, ktorá obsahuje najnovšiu verziu Adobe Flash Player. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko bolo zaznamenané použitie exploitov na niektoré uvedené zraniteľnosti.
Správcom systémov odporúčame prezrieť si novembrové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-130.aspx
https://technet.microsoft.com/en-us/library/security/ms16-131.aspx
https://technet.microsoft.com/en-us/library/security/ms16-132.aspx
https://technet.microsoft.com/en-us/library/security/ms16-135.aspx
https://technet.microsoft.com/en-us/library/security/ms16-141.aspx

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosti CVE-2016-7213, CVE-2016-7228, CVE-2016-7229, CVE-2016-7230, CVE-2016-7231, CVE-2016-7232, CVE-2016-7234, CVE-2016-7235, CVE-2016-7236 a CVE-2016-7237 sú spôsobené chybami pri práci s objektmi v pamäti. Umožňujú vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení infikovaného dokumentu.

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 edition)
Microsoft Office 2016 (64-bit edition)

Microsoft Office for Mac 2011
Microsoft Office 2016 for Mac
Microsoft Excel Viewer
Microsoft PowerPoint Viewer

Microsoft Office Compatibility Pack Service Pack 3

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 MS16-133. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré z uvedených zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si novembrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-133.aspx

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na 7 zraniteľností, z ktorých sú 4 označené ako kritické, sú spôsobené chybami pri práci s pamäťou a umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej stránky.

Zraniteľné systémy:
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 MS16-142. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré z uvedených zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si novembrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-142.aspx

Microsoft Edge

Spoločnosť Microsoft vydala sadu záplat na 17 zraniteľností, z ktorých je 11 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 MS16-129. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedené zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si novembrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-129.aspx

Mozilla Firefox

Spoločnosť Mozilla vydala tri aktualizácie prehliadača Firefox opravujúce dokopy 5 kritických zraniteľností umožňujúcich vzdialené spustenie škodlivého kódu, spôsobiť pád aplikácie alebo obchádzanie bezpečnostných mechanizmov, prípadne ďalšie bližšie nešpecifikované dopady po navštívení infikovaných webstránok.

Opravená bola aj zraniteľnosť CVE-2016-9079 v komponente SVG Animation, ktorá bola aktívne zneužívaná útočníkmi.

Zraniteľné systémy:
Mozilla Firefox 50.0.1 a predchádzajúce
Mozilla Firefox ESR 45.5.0

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 50.0.2, resp. Mozilla Firefox ESR 45.5.1).
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 následne stiahnu aktualizácie.

Zdroje:
https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=150
https://www.mozilla.org/en-US/security/advisories/mfsa2016-89/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-90/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-91/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-92/

Google Chrome

Spoločnosť Google zverejnila dve aktualizácie prehliadača Chrome, ktoré obsahujú opravy 5 bezpečnostných zraniteľností.

Najvážnejšie zraniteľnosti umožňujú spôsobiť pád aplikácie, XSS, únik citlivých informácií alebo iný, bližšie nešpecifikovaný dopad po načítaní infikovaných webstránok alebo otvorení infikovaného PDF súboru.

Zraniteľné systémy
Google Chrome verzie 54.0.2840.100 a nižšej

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 55.0.2883.75. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
https://googlechromereleases.blogspot.sk/2016/11/stable-channel-update-for-desktop.html
https://googlechromereleases.blogspot.sk/2016/11/stable-channel-update-for-desktop_9.html
https://googlechromereleases.blogspot.sk/2016/12/stable-channel-update-for-desktop.html

4. Adobe Flash Player

Spoločnosť Adobe zverejnila jednu aktualizáciu opravujúcu 9 zraniteľností, všetky sú označené ako kritické.

Zraniteľnosti sú spôsobené použitím nesprávnych typov premenných a opätovným použitím uvoľnenej pamäte. Tieto zraniteľnosti umožňujú vzdialenému útočníkovi spustiť škodlivý kód pomocou infikovaného Flash obsahu.

Zraniteľné systémy:
Adobe Flash Player verzie 23.0.0.205 a nižšej
Adobe Flash Player verzie 11.2.202.643 a nižšej

Odporúčania:
Používateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 23.0.0.207, používateľom Linux odporúčame aktualizovať na verziu 11.2.202.644.
Aktualizáciu odporúčame vykonať čo najskôr, nakoľko bol zaznamenaný výskyt exploitov na niektoré uvedené zraniteľnosti.
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/apsb16-37.html

5. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft v mesiaci november nezverejnila opravy žiadnych zraniteľností platformy .NET.

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

Oracle Java

Spoločnosť Oracle v mesiaci september nevydala žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 17. január 2017.

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