Mesačný prehľad kritických zraniteľností
Október 2016

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2016-3393 vo Windows GDI je spôsobená chybami pri práci s objektmi v pamäti. 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.

Zraniteľnosť CVE-2016-3396 vo Windows GDI+ je spôsobená chybami pri práci Windows Font Library s vloženými fontami. Umožňuje vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení infikovaného dokumentu. Útočník môže zneužitím tejto zraniteľnosti prevziať kontrolu nad zariadením.

Zraniteľnosť CVE-2016-0142 v komponente Microsoft Video Control je spôsobená chybami pri práci s objektmi v pamäti. Umožňuje vzdialené spustenie škodlivého kódu po otvorení infikovaného dokumentu.

Zároveň spoločnosť Google publikovala informácie o doteraz neopravenej kritickej zraniteľnosti v komponente Win32k. Zraniteľnosť je možné zneužiť na zvýšenie privilégií a 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 8.1 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)

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označeniami MS16-120, MS16-116 a taktiež aj MS16-117, ktorá obsahuje najnovšiu verziu Adobe Flash Player. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko bolo zaznamenané použitie exploitov na niektoré uvedené zraniteľnosti. Taktiež odporúčame pravidelne sledovať dostupnosť aktualizácií alebo odporúčaní spoločnosti Microsoft ohľadne dosiaľ neopravenej zraniteľnosti.
Správcom systémov odporúčame prezrieť si októbrové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-120.aspx
https://technet.microsoft.com/en-us/library/security/ms16-122.aspx
https://technet.microsoft.com/en-us/library/security/ms16-127.aspx
https://technet.microsoft.com/en-us/library/security/ms16-128.aspx
https://security.googleblog.com/2016/10/disclosing-vulnerabilities-to-protect.html

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosť CVE-2016-7193 je spôsobená chybami pri spracovaní RTF dokumentov. Umožňuje vzdialené spustenie škodlivého kódu s právami prihláseného používateľa po otvorení infikovaného súboru. Bolo zaznamenané zneužitie tejto zraniteľnosti útočníkmi.

Zraniteľnosť CVE-2016-3393 vo Windows GDI je spôsobená chybami pri práci s objektmi v pamäti. 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.

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 Word 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
Office Online Server

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS16-107. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko bol zaznamenaný výskyt exploitov na niektoré uvedené zraniteľnosti.
Správcom systémov odporúčame prezrieť si októbrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-120.aspx
https://technet.microsoft.com/en-us/library/security/ms16-121.aspx

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na 11 zraniteľností, z ktorých je 6 označených ako kritických, sú spôsobené chybami pri práci s pamäťou a umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej stránky.

Zraniteľnosť CVE-2016-3298 je spôsobená chybami pri práci s objektmi v pamäti a umožňuje vzdialenému útočníkovi testovanie prítomnosti súborov na disku zariadenia po navštívení infikovanej webstránky. Bolo zaznamenané zneužitie tejto zraniteľnosti útočníkmi.

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 MS16-118. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko bol zaznamenaný výskyt exploitov na niektoré uvedené zraniteľnosti. Správcom systémov odporúčame prezrieť si októbrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-118.aspx

Microsoft Edge

Spoločnosť Microsoft vydala sadu záplat na 13 zraniteľností, z ktorých je 8 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 MS16-119. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedené zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si októbrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-119.aspx

Mozilla Firefox

Spoločnosť Mozilla vydala jednu aktualizáciu prehliadača Firefox opravujúcu 2 vážne zraniteľnosti umožňujúce spôsobiť pád aplikácie alebo únik citlivých informácií, prípadne ďalšie bližšie nešpecifikované dopady. Kritické zraniteľnosti neboli opravené žiadne.

Zraniteľné systémy:
Mozilla Firefox 49.0.1 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 49.0.2). 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/en-US/security/advisories/mfsa2016-87/

Google Chrome

Spoločnosť Google zverejnila dve aktualizácie prehliadača Chrome, ktoré obsahujú opravy 21 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 54.0.2840.71 a nižšej

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 54.0.2840.87. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
https://googlechromereleases.blogspot.sk/2016/10/stable-channel-update-for-desktop.html
https://googlechromereleases.blogspot.sk/2016/10/stable-channel-update-for-desktop_20.html
https://googlechromereleases.blogspot.sk/2016/11/stable-channel-update-for-desktop.html

4. Adobe Flash Player

Spoločnosť Adobe zverejnila dve aktualizácie opravujúce 13 zraniteľností, všetky sú označené ako kritické.

Zraniteľnosti sú spôsobené použitím nesprávnych typov premenných, opätovným použitím uvoľnenej pamäte, chybami pri práci s objektami v pamäti a ďalšími chybami. Tieto zraniteľnosti umožňujú vzdialenému útočníkovi spustiť škodlivý kód alebo únik informácií pomocou infikovaného Flash obsahu. Bolo zaznamenané použitie exploitov na zraniteľnosť CVE-2016-7855.

Zraniteľné systémy:
Adobe Flash Player verzie 23.0.0.185 a nižšej
Adobe Flash Player verzie 18.0.0.375 a nižšej
Adobe Flash Player verzie 11.2.202.637 a nižšej

Odporúčania:
Používateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 23.0.0.205, používateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu 18.0.0.382. Používateľom Linux odporúčame aktualizovať na verziu 11.2.202.643.
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/apsb16-32.html
https://helpx.adobe.com/security/products/flash-player/apsb16-36.html

5. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft v mesiaci október nevydala opravy žiadnych kritických zraniteľností platformy .NET. Boli však zverejnené dôležité aktualizácie opravujúce zraniteľnosť CVE-2016-3209 umožňovala únik citlivých informácií a obídenie ochrany ASLR.

Zraniteľné systémy:
Microsoft .NET Framework 3.0 Service Pack 2
Microsoft .NET Framework 3.5/3.5.1
Microsoft .NET Framework 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 MS16-120. Odporúčame všetkým používateľom aktualizovať zraniteľný softvér. Správcom systémov odporúčame prezrieť si októbrový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-120.aspx

Oracle Java

Spoločnosť Oracle v mesiaci október vydala bezpečnostnú aktualizáciu platformy Java opravujúcu 13 zraniteľností, z ktorých je 5 kritických.

Zraniteľnosti CVE-2016-5556, CVE-2016-5568, CVE-2016-5582 a CVE-2016-5573 umožňujú vzdialenému útočníkovi bez autentifikácie spustenie škodlivého kódu, kompromitáciu zariadenia, alebo iné bližšie neurčené dopady.

Zraniteľné systémy:
Java SE 6u121
Java SE 7u111
Java SE 8u102

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 111.

Zdroje:
http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html

6. Iné závažné zraniteľnosti

Zraniteľnosť Dirty COW v Linuxovom jadre

Zraniteľnosť CVE-2016-5195 je spôsobená chybou v subsystéme pre správu pamäte. Pri súbehu viacerých vlákien je možné prostredníctvom Copy-on-Write (COW) dosiahnuť zápis do pamäťových stránok a súborov, ktoré sú určené iba na čítanie. Útočník môže zraniteľnosť

využiť na vloženie vlastného obsahu do súborov, ku ktorým by nemal mať prístupové práva na zápis.
Zverejnený exploit zneužíva zraniteľnosť, prostredníctvom ktorej môžu útočníci získať oprávnenia správcu (root-a) po spustení škodlivého programu. Je pravdepodobné, že uvedená zraniteľnosť bola už nejaký čas aktívne zneužívaná útočníkmi.

Zraniteľné systémy:
Linux Kernel 2.6.22 a novší

Odporúčania:
18.10.2016 bola zverejnená oprava uvedenej zraniteľnosti a postupne je distribuovaná s opravenými jadrami v hlavných Linuxových distribúciach. Administrátorom odporúčame čo najskôr aktualizovať jadro, nakoľko exploit na uvedenú zraniteľnosť je verejne dostupný.

Zdroje:
https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails