Mesačný prehľad kritických zraniteľností Jún 2015

1.Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2015-1728 prehrávača Windows Media Player umožňuje spustenie škodlivého kódu po otvorení multimediálneho obsahu v aplikácii. Vzdialený útočník môže túto zraniteľnosť zneužiť prostredníctvom e-mailov s infikovanou prílohou alebo webstránok so škodlivým obsahom pre Windows Media Player, ak užívateľ tento obsah zobrazí.

Zraniteľnosť CVE-2015-2360 vo Windows kernel-mode driver (Win32k.sys) spôsobená nesprávnym uvoľnovaním nepoužívanej pamäte. Útočník prihlásený do systému môže zneužiť túto zraniteľnosť na spustenie programov s oprávneniami iného používateľa. Prostredníctvom tejto zraniteľnosti teda je útočník schopný v niektorých prípadoch spustiť program s právami administrátora a prevziať kontrolu nad zariadením. Na túto zraniteľnosť už boli zaznamenané exploity.

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 RT
Windows RT 8.1
Windows Server 2003 Service Pack 2
Windows Server 2003 x64 Edition Service Pack 2
Windows Server 2003 with SP2 for Itanium-based Systems
Windows Server 2003 R2 Service Pack 2
Windows Server 2003 R2 x64 Edition Service Pack 2
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 MS15-057 a MS15-061. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti už sú používané pri útokoch. Správcom systémov odporúčame prezrieť si júnové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/library/security/MS15-057
https://technet.microsoft.com/library/security/MS15-061

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosti CVE-2015-1759 a CVE-2015-1760 spôsobené chybami pri práci s objektmi v pamäti počas spracovania dokumentov Office umožňuje útočníkovi vzdialené spustenie škodlivého kódu s oprávneniami užívateľa, ktorý otvorí infikovaný súbor.

Zraniteľnosť CVE-2015-1770 spôsobená použitím neinicializovanej pamäte počas spracovania dokumentov Office umožňuje útočníkovi vzdialené spustenie škodlivého kódu s oprávneniami užívateľa, ktorý otvorí infikovaný súbor.

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

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS15-059. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré zraniteľnosti je pravdepodobný.
Správcom systémov odporúčame prezrieť si júnové Microsoft Security Bulletin dostupné na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/library/security/MS15-059

3.Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na zraniteľnosti, z ktorých 20 je označených ako kritických, väčšina je spôsobená chybami pri práci s pamäťou a umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej stránky.

Zraniteľné systémy:
Microsoft Internet Explorer 6-11

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS15-089. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si júnový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/library/security/MS15-056

Mozilla Firefox

Spoločnosť Mozilla vydala v mesiaci jún jednu minoritnú aktualizáciu prehliadača Firefox vylepšujúcu grafický výkon verzie pre Windows 7 a integráciu služby Pocket. Neboli zverejnené žiadne bezpečnostné opravy.

Odporúčania:
Užívatelia môžu aktualizovať prehliadač na najnovšiu verzie 38.0.5.
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/en-US/firefox/38.0.5/releasenotes/

Google Chrome

Spoločnosť Google vydala tri aktualizácie prehliadača Chrome, ktoré obsahujú opravy bezpečnostných zraniteľností a taktiež obsahujú novú verziu Adobe Flash Player.

Zraniteľnosť CVE-2015-1266 umožňuje obísť obmedzenie prístupu vynútením nesprávnej schémy pri podobných URL adresách (napr. http://gpu a chrome://gpu).

Zraniteľnosť CVE-2015-1268 umožňuje obísť kontrolu Same Origin Policy v jadre Blink pomocou škodlivého JavaScript kódu.

Zraniteľné systémy
Google Chrome do verzie 43.0.2357.130

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 43.0.2357.130, nakoľko exploit na niektoré zraniteľnosti Flash Playera už je používaný. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://googlechromereleases.blogspot.in/2015/06/stable-channel-update.html
http://googlechromereleases.blogspot.sk/2015/06/stable-channel-update_11.html
http://googlechromereleases.blogspot.in/2015/06/chrome-stable-update.html

4.Adobe Flash Player

Spoločnosť Adobe vydala v mesiaci jún dve aktualizácie opravujúce 14 zraniteľností. Väčšina zraniteľnosti je spôsobená rôznymi chybami pri práci s pamäťou. Zraniteľnosti umožňujú vzdialenému útočníkovi spustenie škodlivého kódu alebo obídenie bezpečnostných prvkov (ASLR, Same Origin Policy).
Na zero-day zraniteľnosť CVE-2015-3090 bol zaznamenaný výskyt exploitu ešte pred zverejnením opravy tejto chyby. Zraniteľnosť je spôsobená pretečením pamäte na halde a jej zneužitie vedie k vzdialenému spusteniu škodlivého kódu.

Zraniteľné systémy
Adobe Flash Player verzie 18.0.0.161 a nižšej
Adobe Flash Player verzie 13.0.0.292 a nižšej
Adobe Flash Player verzie 11.2.202.466 a nižšej

Odporúčania:
Užívateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 18.0.0.194, užívateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu 13.0.0.296. Užívateľom Linux odporúčame aktualizovať na verziu 11.2.202.468. Aktualizáciu odporúčame vykonať čo najskôr, nakoľko bolo zaznamenané použitie exploitov na niektoré zraniteľnosti.
Aktualizácie sú dostupné prostredníctvom stránky Adobe Flash Player Download Center, prípadne prostredníctvom kontroly dostupných aktualizácii v produkte Adobe Flash Player 18.x.

Zdroje:
https://helpx.adobe.com/security/products/flash-player/apsb15-11.html
https://helpx.adobe.com/security/products/flash-player/apsb15-14.html

5.Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft v mesiaci jún nevydala žiadne bezpečnostné aktualizácie platformy .NET.

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

Oracle Java

Spoločnosť Oracle v mesiaci jún nevydala žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 14. júl 2015.

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

6.Iné závažné zraniteľnosti

Antivírusový program ESET

V produkte firmy ESET bola identifikovaná zraniteľnosť umožňujúca spustenie ľubovoľného kódu s právami administrátora. Vzdialený útočník je schopný podvrhnúť súbor, ktorý pri skenovaní antivírovým riešením ESET spustí kód vložený útočníkom. Kód je spustený s právami administrátora.

Zraniteľné systémy:
Všetky podporované verzie ESET

Odporúčania:
Odporúčame nainštalovať aktualizáciu programových modulov vydanou spoločnosťou ESET 22.6.2015.

Zdroje:
http://googleprojectzero.blogspot.cz/2015/06/analysis-and-exploitation-of-eset.html
https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=136

CISCO bezpečnostný softvér

Spoločnosť Cisco vydala opravu svojich produktov Virtual WSA (Web Security Appliances), ESA (Email Security Appliances) a SMA (Security Management Appliances). Uvedené produkty obsahovali prednastavené rovnaké verejné SSH kľúče určené pre vzdialenú podporu. Po získaní privátnych kľúčov mohol vzdialený útočník dešifrovať alebo meniť komunikáciu s jednotlivými produktmi.

Zraniteľné systémy:
Cisco Content Security Management Virtual Appliance 8.4.0.0150, 9.0.0.087
Cisco Email Security Virtual Appliance 8.0.0, 8.5, 8.6, 8.7, 9.0.0, 9.1.0
Cisco Web Security Virtual Appliance 7.7.5, 8.0.5, 8.5.0, 8.5.1, 8.6 .0, 8.7.0

Odporúčania:
Spoločnosť Cisco vydala opravu uvedenej zraniteľnosti, zákazníci s aktívnym kontraktom môžu získať aktualizácie prostredníctvom Software Center (https://software.cisco.com/download/navigator.html).
Zákazníci bez kontraktu by mali kontaktovať zákaznícku podporu.

Zdroje:
http://tools.cisco.com/security/center/viewAlert.x?alertId=39461