Mesačný prehľad kritických zraniteľností August 2015

1. Operačné systémy Microsoft Windows

Zraniteľnosti CVE-2015-2432, CVE-2015-2458, CVE-2015-2459, CVE-2015-2460, CVE-2015-2461 a CVE-2015-2462 v knižnici Adobe Type Manager sú spôsobené chybami pri spracovaní OpenType fontov. Umožňujú vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení dokumentu obsahujúceho infikované OpenType fonty. Útočník zneužitím tejto zraniteľnosti môže získať systémové práva a prevziať kontrolu nad zariadením.

Zraniteľnosti CVE-2015-2435, CVE-2015-2455, CVE-2015-2456, CVE-2015-2463 a CVE-2015-2464 v knižnici Windows DirectWrite sú spôsobené chybami pri spracovaní TrueType fontov. Umožňujú vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení dokumentu obsahujúceho infikované TrueType fonty. Útočník zneužitím tejto zraniteľnosti môže získať systémové práva a prevziať kontrolu nad zariadením.

Zraniteľnosť CVE-2015-1769 v komponente Mount Manager je spôsobená nesprávnym spracovávaním symbolických odkazov. Umožňuje útočníkovi s fyzickým prístupom k zariadeniu po vložení infikovaného USB zariadenia zapísať na disk škodlivý program a následne ho spustiť. Bolo zaznamenané použitie exploitov na túto zraniteľnosť.

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 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 MS15-080 a MS15-085. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko exploity na niektoré zraniteľnosti sú verejne známe a použitie exploitov na ostatné zraniteľnosti je pravdepodobné.

Pokiaľ používate produkty Windows Server 2003, odporúčame prejsť na novšiu verziu Windows Server 2012, pretože verzia 2003 už nie je ďalej podporovaná.
Správcom systémov odporúčame prezrieť si augustové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/library/security/MS15-080
https://technet.microsoft.com/library/security/MS15-085
http://www.microsoft.com/en-us/server-cloud/products/windows-server-2003/

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosť CVE-2015-1642 spôsobená chybami pri práci s objektmi v pamäti umožňuje útočníkovi vzdialené spustenie škodlivého kódu s oprávneniami užívateľa, ktorý otvorí infikovaný súbor. Bolo zaznamenané použitie exploitov na túto zraniteľnosť.

Zraniteľnosť CVE-2015-2466 spôsobená nesprávnou validáciou šablón Microsoft Office umožňuje útočníkovi vzdialené spustenie škodlivého kódu s oprávneniami užívateľa, ktorý otvorí infikovanú šablónu.

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 for Mac 2011
Microsoft Office for Mac 2016
Microsoft Word Viewer
Microsoft Excel Viewer 2007 Service Pack 3
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
Microsoft Office Web Apps 2013

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS15-081. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko bol zaznamenaný výskyt exploitov na zraniteľnosť CVE-2015-2466.
Správcom systémov odporúčame prezrieť si augustový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/library/security/MS15-081

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala dve sady záplat na zraniteľnosti, z ktorých 11 je označených ako kritických, sú spôsobené chybami pri práci s pamäťou 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 označeniami MS15-079 a MS15-093. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko bol zaznamenaný výskyt exploitu na zraniteľnosť CVE-2015-2502 a výskyt exploitov na niektoré iné zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si augustové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroj:
https://technet.microsoft.com/library/security/MS15-079
https://technet.microsoft.com/library/security/MS15-093
http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=138

Mozilla Firefox

Spoločnosť Mozilla vydala v mesiaci august štyri aktualizácie prehliadača Firefox opravujúce dokopy 83 zraniteľností, z toho je 11 označených ako kritických.

Zraniteľnosť CVE-2015-4495 vstavaného PDF prehliadača umožňuje obísť zabezpečenie Same Origin Policy a vložiť JavaScriptový kód, ktorý môže prechádzať, čítať a odosielať súbory na zariadení používateľa. Exploity na túto zraniteľnosť sú verejne dostupné.

Zraniteľnosť CVE-2015-4477 spôsobená opätovným použitím uvoľnenej pamäte umožňuje vzdialené spustenie škodlivého kódu prostredníctvom Web Audio API.

Zraniteľnosti CVE-2015-4479, CVE-2015-4480, CVE-2015-4493 a CVE-2015-4496 spôsobené pretečením pamäte (buffer overflow), prípadne pretečením rozsahu celočíselných premenných (integer overflow) umožňujú vzdialené spustenie škodlivého kódu pri spracovaní videa vo formáte MPEG4.

Zraniteľnosti CVE-2015-4485 a CVE-2015-4486 spôsobené pretečením pamäte (buffer overflow) umožňujú vzdialené spustenie škodlivého kódu pri spracovaní videa vo formáte WebM.

Zraniteľnosť CVE-2015-4497 spôsobená opätovným použitím uvoľnenej pamäte umožňuje vzdialené spustenie škodlivého kódu pri narábaní s elementom canvas.

Zraniteľnosti CVE-2015-4473, CVE-2015-4474 spôsobené bližšie nešpecifikovanými chybami pri práci s pamäťou môžu viesť k vzdialenému spusteniu škodlivého kódu.

Zraniteľné systémy:
Mozilla Firefox 40.0.2 a predchádzajúce
Mozilla Firefox ESR 38.2.0 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 40.0.3 a Mozilla Firefox ESR 38.2.1)
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.mozilla.org/sk/security/advisories/
http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=137

Google Chrome

Spoločnosť Google vydala štyri aktualizácie prehliadača Chrome, ktoré obsahujú opravy 29 bezpečnostných zraniteľností.

Najvážnejšie zraniteľnosti sú spôsobené najmä chybami pri práci s pamäťou (znovupoužitie uvoľnenej pamäte) a umožňujú spôsobiť pád aplikácie, prípadne obísť zabezpečenie Same-origin-policy (Cross-origin bypass).

Zraniteľné systémy
Google Chrome do verzie 45.0.2454.85

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 45.0.2454.85. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://googlechromereleases.blogspot.in/2015/08/stable-channel-update.html
http://googlechromereleases.blogspot.in/2015/08/stable-channel-update_11.html
http://googlechromereleases.blogspot.in/2015/08/stable-channel-update_20.html
http://googlechromereleases.blogspot.in/2015/09/stable-channel-update.html

4. Adobe Flash Player

Spoločnosť Adobe vydala aktualizáciu opravujúcu 35 zraniteľnosti, všetky sú označené ako kritické.

Zraniteľnosti sú spôsobené opätovným použitím uvoľnenej pamäte, pretečením pamäte (buffer overflow), pretečením rozsahu celočíselných premenných (integer overflow), použitím nesprávnych typov premenných a ďalšími chybami pri práci s pamäťou. Tieto zraniteľnosti umožňujú vzdialenému útočníkovi spustiť škodlivý kód pomocou infikovaného Flash obsahu.

Zraniteľné systémy
Adobe Flash Player verzie 18.0.0.209 a nižšej
Adobe Flash Player verzie 13.0.0.309 a nižšej
Adobe Flash Player verzie 11.2.202.491 a nižšej

Odporúčania:
Užívateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 18.0.0.232, užívateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať taktiež na verziu 18.0.0.232, ktorá je novou verziou s predĺženou podporou. Užívateľom Linux odporúčame aktualizovať na verziu 11.2.202.508.
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/apsb15-19.html

5. Frameworky

Microsoft .NET Framework

Zraniteľnosti CVE-2015-2460 a CVE-2015-2462 v knižnici Adobe Type Manager sú spôsobené chybami pri spracovaní OpenType fontov. Umožňujú vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení dokumentu obsahujúceho infikované OpenType fonty. Útočník zneužitím tejto zraniteľnosti môže získať systémové práva a prevziať kontrolu nad zariadením.

Zraniteľnosti CVE-2015-2455, CVE-2015-2456, CVE-2015-2463 a CVE-2015-2464 v knižnici Windows DirectWrite sú spôsobené chybami pri spracovaní TrueType fontov. Umožňujú vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení dokumentu obsahujúceho infikované TrueType 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 MS15-080. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré iné zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si augustové Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/library/security/MS15-080

Oracle Java
Spoločnosť Oracle v mesiaci jún nevydala žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 20. október 2015.

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

6. Iné závažné zraniteľnosti
Certifi-Gate
Skupina zraniteľností zariadení so systémom Android. Zraniteľnosti sa nachádzajú v autorizačných metódach aplikácií používaných pre vzdialenú technickú podporu používateľov. Technická podpora môže pomocou Remote Support Tool zobraziť obrazovku zariadenia a simulovať kliknutia a dotyky. Zraniteľnosti Certifi-Gate môžu byť zneužité škodlivými aplikáciami na získanie neoprávneného privilegovaného prístupu do zariadenia a ku všetkým užívateľským údajom a prostredníctvom nástrojov pre vzdialenú podporu, ktoré sú v prístroji predinštalované výrobcom, prípadne operátorom.

V obchode Google Play sa už objavila aplikácia nazvaná Easy Screen recorder No Root, ktorá zneužíva uvedenú zraniteľnosť na zachytávanie videa z obrazovky zariadenia.

Zraniteľné systémy:
Android 4.4 a 5.0

Spoločnosť CheckPoint zverejnila na Google Play aplikáciu, pomocou ktorej je možné otestovať zraniteľnosť Vášho zariadenia:
https://play.google.com/store/apps/details?id=com.checkpoint.capsulescanner

Odporúčania:
Zraniteľnosti Certifi-Gate nie je možné jednoducho opraviť, pretože systém Android neponúka možnosť revokovať certifikáty, ktorými sú podpísané komponenty systému umožňujúce získať privilegované oprávnenia.
Používateľom zraniteľných zariadení na zmiernenie rizika odporúčame neinštalovať nedôveryhodné aplikácie, pravidelne aktualizovať nainštalované aplikácie aj operačný systém a pokiaľ je to možné, odinštalovať alebo zakázať nástroje pre vzdialenú podporu používateľov.

Zdroje:
http://blog.checkpoint.com/2015/08/06/certifigate/
http://www.ibtimes.co.uk/certifi-gate-massive-android-vulnerability-affects-hundreds-millions-smartphones-tablets-1514398
http://www.ibtimes.co.uk/certifi-gate-android-bug-exploited-by-hackers-through-app-found-google-play-store-1517019