Mesačný prehľad kritických zraniteľností

Máj 2017

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft v máji vydala aktualizácie na opravu viacerých kritických zraniteľností v protokole SMBv1 (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278 a CVE-2017-0279 – iné ako v marcovom bulletine MS17-010), ktoré neautentifikovanému útočníkovi umožňujú na diaľku vykonať škodlivý kód zaslaním špeciálne pripraveného paketu. Aj neúspešný útok môže spôsobiť obmedzenie dostupnosti systému.

V máji vydala spoločnosť Microsoft opravu kritickej zraniteľnosti CVE-2017-0290 v Microsoft Malware Protection Engine, ktorá umožňuje útočníkovi na diaľku vykonať škodlivý kód s právomocami LocalSystem. To je možné spôsobením narušenia integrity pamäte po preskenovaní špeciálne pripraveného súboru, dopraveného na cieľový počítač ľubovoľným spôsobom. Dôkaz existencie tejto zraniteľnosti je verejne dostupný. CSIRT.SK vydal ku tejto zraniteľnosti dňa 12.05.2017 varovanie, v ktorom je možné nájsť ďalšie podrobnosti (odkaz nižšie).

Koncom mája vydala spoločnosť Microsoft mimoriadne aj druhý balík opráv pre ďalšie kritické zraniteľnosti v Microsoft Malware Protection Engine (CVE-2017-8538, CVE-2017-8540, CVE-2017-8541 a ďalšie), ktoré podobne ako zraniteľnosť CVE-2017-0290 umožňujú vzdialené vykonanie škodlivého kódu, prípadne odopretie služby (DoS), taktiež po preskenovaní špeciálne vytvoreného súboru.

Spločnosť Microsoft tiež vydala vyše 600 opráv zraniteľností, označených ako dôležité. Za zmienku stoja zraniteľnosti CVE-2017-0175, CVE-2017-0220, CVE-2017-0245, CVE-2017-0258 a CVE-2017-0259, na ktoré sú verejne dostupné exploity a ktoré môžu zapríčiniť únik informácií kvôli chybe v jadre systému Windows pri inicializácii objektov v pamäti.

V máji bola objavená chyba v súborovom systéme NTFS, ktorá útočníkovi bez akýchkoľvek oprávnení umožuje spôsobiť obmedzenie dostupnosti zariadenia. To je možné použitím špeciálneho volania pre prístup ku fiktívnemu súboru, pričom cesta ku tomuto súboru obsahuje aj súbor $MFT (Master File Table), ale v roli priečinka. Systém NTFS fiktívny súbor nenájde a pri pokuse uzavrieť “priečinok“ $MFT zlyhá, keďže tento súbor je otvorený a zamknutý samotným NTFS systémom. Vzhľadom na to, že funkcia vykonávajúca pôvodné volanie na otvorenie fiktívneho súboru očakáva zatvorenie a uvoľnenie “priečinku“ $MFT, dochádza ku zamrznutiu danej partície a v prípade systémovej partície aj celého systému. Na obnovenie funkčnosti je potrebný reštart systému. Útočník môže prístup na takýto fiktívny súbor umiestniť napríklad na webovú stránku. V čase písania tohto prehľadu chyba nie je opravená.

Zraniteľné systémy:

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 RT 8.1
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 10 Version 1703 for 32-bit Systems
Windows 10 Version 1703 for x64-based Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012
Windows Server 2012 R2

Windows Server 2016

Microsoft Malware Protection Engine verzie 1.1.13704.0 a starších, ako súčasť softvérov:

- Microsoft Forefront Endpoint Protection 2010
- Microsoft Forefront Security for SharePoint Service Pack 3
- Microsoft Security Essentials
- Microsoft System Center Endpoint Protection
- Microsoft Endpoint Protection
- Microsoft Forefront Endpoint Protection
- Microsoft Forefront Endpoint Protection 2010
- Windows Defender for Windows 7
- Windows Defender for Windows 8.1
- Windows Defender for Windows RT 8.1
- Windows Defender for Windows 10
- Windows Defender for Windows 10 1511
- Windows Defender for Windows 10 1607
- Windows Defender for Windows 10 1703
- Windows Defender for Windows Server 2016
- Windows Intune Endpoint Protection
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016

Odporúčania:

Odporúčame deaktivovať protokol SMBv1 (návod na druhom odkaze). Taktiež odporúčame preveriť, či prebehla automatická aktualizácia Microsoft Malware Protection Engine na verziu 1.1.13804.0 alebo novšiu a v prípade potreby ju spustiť manuálne. Okrem toho odporúčame aplikovať aktualizácie pre systémy Windows, publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania.

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0272
https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=153
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0290
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8541
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0175
http://techreport.com/news/31981/ntfs-filesystem-bug-could-crash-windows-7-8-and-8-1?post=1037908#1037908

2. Kancelárske balíky Microsoft Office a Office Web Apps

V rámci májového balíka aktualizácií spoločnosť Microsoft vydala opravy zero-day zraniteľností CVE-2017-0261 a CVE-2017-0262, ktoré útočníkovi prostredníctvom špeciálne upraveného EPS súboru umožňujú na diaľku prevziať kontrolu nad systémom a na diaľku vykonať škodlivý kód. Pre úspešné zneužitie zraniteľnosti musí používateľ súbor najskôr sám otvoriť, bez ohľadu na to, či sa súbor na počítač dostal z webstránky alebo prílohou v emaili. V čase zverejnenia aktualizácie už bolo zaznamenané zneužitie týchto zraniteľností.

Zraniteľné systémy:

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).

Odporúčania:

Aplikovať balíky aktualizácií, publikované prostredníctvom služby Windows Update, nakoľko zraniteľnosti už sú útočníkmi zneužívané. Číslo aktualizácie pre konkrétnu verziu možno vyhľadať navštívením prvého z nižšie uvedených odkazov a vložením identifikátora zraniteľnosti do vyhľadávania.

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0261
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0262

3. Internetové prehliadače

Microsoft Internet Explorer

V rámci májového balíka aktualizácií bola spoločnosťou Microsoft vydaná oprava zero-day zraniteľnosti CVE-2017-0222 v IE10 a IE11, ktorá umožnuje útočníkovi na ďiaľku vykonať škodlivý kód s právomocami práve prihláseného používateľa. Zraniteľnosť spočíva v chybe v prístupe ku objektu v pamäti, čo má za následok narušenie integrity pamäte. Na zneužitie zraniteľnosti musí používateľ navštíviť špeciálne vytvorenú webovú stránku so škodlivým obsahom alebo otvorením škodlivej prílohy v emaili. Zneužitie tejto zraniteľnosti už bolo zaznamenané.

Taktiež bola vydaná oprava kritickej zraniteľnosti CVE-2017-0228 v skriptovacom engine JavaScript, kde vďaka chybe pri narábaní s objektami v pamäti môže dôsť ku narušeniu integrity pamäte. Na úspešné zneužitie zraniteľnosti musí používateľ navštíviť špeciálne pripravenú stránku, prípadne stránku s umiesteným škodlivým obsahom, v dôsledku čoho získa útočník možnosť vzdialeného vykonania škodlivého kódu s právomocami daného používateľa.

Zraniteľné systémy:
Microsoft Internet Explorer 10
Microsoft Internet Explorer 11

Odporúčania:
Odporúčame používateľom a správcom čo najskôr aplikovať aktualizácie cez službu Windows Update. Číslo aktualizácie pre konkrétnu verziu možno vyhľadať navštívením prvého z nižšie uvedených odkazov a vložením identifikátora zraniteľnosti do vyhľadávania.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0222
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0228

Microsoft Edge

Májový balík aktualizácií pre Microsoft Edge ošetruje kritickú zraniteľnosť CVE-2017-0221, umožňujúcu spôsobiť narušenie integrity pamäte zneužitím chyby v narábaní s objektom v pamäti. Útočník môže presvedčiť používateľa navštíviť špeciálne pripravenú stránku, prípadne inú stránku s umiestneným škodlivým obsahom a následne a diaľku vykonať škodlivý kód s právomocami daného používateľa.

Okrem toho boli vydané opravy na ďalších deväť kritických zraniteľností CVE-2017-0223, CVE-2017-0224, CVE-2017-0227, CVE-2017-0228, CVE-2017-0229, CVE-2017-0235, CVE-2017-0236, CVE-2017-0240 a CVE-2017-0266, ktoré všetky umožňujú útočníkovi vzdialené vykonanie škodlivého kódu s právomocami používateľa vďaka spôsobeniu narušenia integrity pamäte. Zraniteľnosti spočívajú v chybách v správe pamäte v komponentoch Microsoft scripting engines, JavaScript a Chakra JavaScript. Pre úspešné zneužitie musí používateľ navštíviť špeciálne pripravenú stránku, prípadne stránku s umiestneným škodlivým obsahom.

Zraniteľné systémy:
Microsoft Edge na systémoch Windows 10 verzií 1511, 1607 a 1730 v 32-bitových aj 64-bitových verziách.

Odporúčania:
Vzhľadom na vysokú pravdepodobnosť výskytu exploitov na uvedené zraniteľnosti odporúčame používateľom a správcom aplikovať balíky aktualizácií, publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétnu verziu možno vyhľadať navštívením uvedeného odkazu a nastavením filtra pre Microsoft Edge.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0221
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0223
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0229

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0235
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0240

Mozilla Firefox

Spoločnosť Mozilla v máji nevydala žiadne aktualizácie pre prehliadač Firefox.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/

Google Chrome

Spoločnosť Google vydala začiatkom mája opravu zraniteľnosti CVE-2017-5068 v komponente WebRTC, v dôsledku ktorej môže dôjsť k súbežným operáciám na zdieľaných zdrojoch. Bližšie detaily ani dôsledky zraniteľnosti neboli verejne publikované.

V mesiaci máj vydala spoločnosť Google aktualizáciu prehliadača Chrome na verziu 58.0.3029.110, ktorá však podľa zverejnených informácií neobsahovala žiadne bezpečnostné opravy.

V máji sa vyskytli správy o možnom útoku na získanie používateľského mena a hashu systémového hesla, prostredníctvom zraniteľnosti v prehliadači Chrome. Zraniteľnosť spočíva vo východzích nastaveniach prehliadača, kde je povolené automatické stiahnutie SCF súboru po tom, ako používateľ navštívi špeciálne pripravenú webovú stránku s pripraveným SCF súborom. Zraniteľnosť čiastočne spočíva aj v spôsobe, ako operačný systém Windows narába s SCF súborom. V okamihu otvorenia priečinku so stiahnutým SCF súborom sa operačný systém pokúsi priradiť stiahnutému súboru ikonu, pričom škodlivý SCF súbor ho odkáže na útočníkov SMB server, v dôsledku čoho operačný systém pri pokuse o pripojenie odošle autentifikačné údaje. Útočníkov server je pripravený odchytiť používateľovo prihlasovacie meno a NTLMv2 hash jeho hesla. Prvým možným dôsledkom je únik hesla v prípade prelomenia hashu. Druhou možnosťou je pre útočníka získanie prístupu do iného systému alebo služby po tom, ako na tento systém prepošle odchytené autentifikačné údaje (SMB Relay útok), v dôsledku čoho môže dôjsť ku úniku dát, alebo ďalším útokom na systém. Spoločnosť Google sa vyjadrila, že si je danej zraniteľnosti vedomá a prijíma potrebné opatrenia.

Zraniteľné systémy:
Google Chrome 58.0.3029.81 a staršie

Odporúčania:
Odporúčame aktualizovať prehliadač Chrome na najnovšiu verziu 58.0.3029.110. Taktiež na zmiernenie rizika vystavenia sa útoku s krádežou prihlasovacích údajov, odporúčame zmeniť nastavenia prehladača Chrome tak, aby vyžadoval povolenie na stiahnutie každého jedného súboru (Nastavenia > Pokročilé nastavenia > Opýtať sa na uloženie každého súboru pred stiahnutím). Správcom sietí tiež odporúčame nastaviť firewall na blokovanie komunikácie cez SMB protokol smerom von zo siete.

Zdroje:
https://chromereleases.googleblog.com/2017/05/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2017/05/stable-channel-update-for-desktop_9.html
https://threatpost.com/chrome-browser-hack-opens-door-to-credential-theft/125686/

4. Adobe Flash Player

Spoločnosť Adobe vydala opravu kritickej zraniteľnosti CVE-2017-3068 v komponente Advanced Video Coding engine, ktorá umožňuje útočníkovi na ďiaľku vykonať škodlivý kód využitím narušenia integrity pamäte v dôsledku čítania mimo vymedzených hraníc. V čase písania tohto mesačníka je na túto zraniteľnosť verejne dostupný exploit.

Ďalšími kritickými zraniteľnosťami sú CVE-2017-3069, CVE-2017-3070, CVE-2017-3071, CVE-2017-3072, CVE-2017-3073 a CVE-2017-3074, v triedach BlendMode, ConvolutionFilter, BitmapData, Graphics a aj pri všobecnej správe objektov v pamäti. Zneužitím týchto chýb môže útočník spôsobiť narušenie integrity pamäte a získať možnosť vykonať na diaľku škodlivý kód.

Zraniteľné systémy:
Adobe Flash Player 25.0.0.148 a staršie

Odporúčania:

Čo najskôr aktualizovať Flash Player na verziu 25.0.0.171, kvôli verejne dostupnému exploitu na prvú menovanú zraniteľnosť. V závislosti od nastavení používateľa sa aktualizácia udeje automaticky alebo zobrazením dialógového okna s upozornením.

Zdroje:
https://helpx.adobe.com/security/products/flash-player/apsb17-15.html

6. Frameworky

Microsoft .NET

Spoločnosť Microsoft v apríli vydala opravu zraniteľnosti CVE-2017-0248 označenej ako dôležitá, ktorá útočníkovi umožňuje obísť bezpečnostné prvky zneužitím chyby pri overovaní certifikátov a následnom použití certifikátu neplatného na daný účel.

Zraniteľné systémy:
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.5/3.5.1
Microsoft .NET Framework 4.5.2
Microsoft .NET Framework 4.6/4.6.1/4.6.2
Microsoft .NET Framework 4.7

Odporúčania:
Aplikovať aktualizácie distribuované prostredníctvom služby Windows Update. Pre zistenie čísla aktualizácie pre váš operačný systém a verziu .NET, navštívte nižšie uvedený odkaz.

Zdroje:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0248

Oracle Java

Spoločnosť Oracle v máji nevydala žiadne aktualizácie. Najbližší balík aktualizácií je plánovaný na 18.7.2017

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

7. Iné závažné zraniteľnosti

Zneužitie uniknutých exploitov Equation Group

V aprílovom prehľade zraniteľností sme informovali o zverejnení uniknutých exploitov od tzv. EquationGroup. Výraznou májovou udalosťou bolo objavenie sa rozsiahlej nákazy ransomvérom WanaCryptor, šíriaci sa prostredníctvom červa, ktorý používa uniknutý exploit EternalBlue. Červ zneužil kritickú zraniteľnosť CVE-2017-0144 v protokole SMBv1, ošetrenú v marcovom Microsoft Security Bulletine MS17-010. CSIRT.SK ku tomuto incidentu vydal varovanie, vrátane odporúčaní na zmiernenie rizika útoku (odkaz nižšie). V druhej polovici mája sa objavil aj červ EternalRocks, ktorý využíva okrem EternalBlue až päť ďalších uniknutých exploitov, avšak doposiaľ nebolo zaznamenané infikovanie systému škodlivým kódom ani po úspešnom preniknutí.

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 RT 8.1
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 Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 64-bit Systems Service Pack 2
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
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016 for x64-based Systems

Výnimočne boli vydané opravy aj pre nepodporované systémy:
Windows XP SP2 x64
Windows XP SP3 x86
Windows 8 x86
Windows 8 x64
Windows Server 2003 SP2 x86
Windows Server 2003 SP2 x64

Odporúčania:
Vzhľadom na existenciu aktuálnych hrozieb a vysokej pravdepodobnosti objavenia sa nových, dôrazne odporúčame aplikovať aktualizácie z Microsoft Security Bulletinu MS17-010 a v prípade potreby aj spomenuté aktualizácie pre staršie systémy. Taktiež odporúčame deaktivovať protokol SMBv1. Správcom sietí odporúčame blokovať pripojenia na port TCP 445 prichádzajúce zvonka siete. Ďalšie informácie a odporúčania možno nájsť vo varovaní na prvom odkaze.

Zdroje:
https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=154
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
https://threatpost.com/wannacry-development-errors-enable-file-recovery/126002/

Samba

V máji bola vydaná oprava na kritickú zraniteľnosť CVE-2017-7494 v softvéri Samba, ktorá útočníkovi umožňovala vykonať na ďiaľku škodlivý kód. Útočníkovi stačí nájsť otvorený SMB systém komunikujúci cez port TCP 445 a s povoleným zapisovaním, nahrať naň súbor so zdieľanou knižnicou a následne primäť server túto knižnicu načítať a vykonať jej kód. Závažným faktom je možnosť zneužtia tejto zraniteľnosti na útoky šíriace sa spôsobom červa. Exploit je v čase písania tohto prehľadu verejne dostupný, pričom údajne je až sto tisíc zariadení so zraniteľnými a nepodporovanými verziami Samba, a portami TCP 445 a TCP 139 otvorenými smerom do internetu.

Zraniteľné systémy:
Samba 3.5.0 a novšie

Odporúčania:
Čo najskôr aktualizovať na opravenú verziu (4.6.4, 4.5.10 alebo 4.4.14 – odkaz nižšie), kvôli vysokému riziku vystavenia sa útoku s možnými vážnymi dôsledkami. V prípade nemožnosti okamžitého aktualizovania na novšiu verziu, odporúčame na zmiernenie rizika v konfiguračnom súbore smb.conf doplniť do sekcie [Global] riadok “nt pipe support = no“ a reštartovať službu. Taktiež odporúčame nastaviť vonkajší firewall na blokovanie komunikácie na porty TCP 445, TCP 139, UDP 137 a UDP 138 smerom z internetu do siete. Jednou z možností zmiernenia rizika je aj obmedzenie práv na zápis do zdieľaných priečinkov.

Zdroje:
https://www.samba.org/samba/security/CVE-2017-7494.html
https://www.samba.org/samba/history/

Zraniteľnosť vo VideoLAN VLC v implementácii parsovania filmových titulkov

Boli identifikované a opravené kritické zraniteľnosti CVE-2017-8310, CVE-2017-8311, CVE-2017-8312 a CVE-2017-8313 vo VideoLAN VLC. Najvážnejšie dôsledky má druhá menovaná zraniteľnosť, kedy útočník môže spôsobením pretečenia zásobníka v komponente ParseJSS vykonať na diaľku ľubovoľný kód a prevziať nad zariadením kontrolu. Zaujímavým novým prvkom je vektor útoku – škodlivý súbor s titulkami. Používateľ musí navštíviť stránku s online prehrávaním videa obsahujúceho škodlivý súbor s titulkami, alebo stiahnuť škodlivý súbor s titulkami na lokálne prehrávanie. Okrem VLC boli takéto zraniteľnosti nájdené aj v prehrávačoch Kodi, Stremio a Popcorn Time a s vysokou pravdepobobnosťou budú nájdené aj v ďalších.

Zraniteľné systémy:
VideoLAN VLC 2.2.4 a staršie

Odporúčania:
Aktualizovať na najnovšiu opravenú verziu prehrávača VLC (2.2.6).

Zdroje:
https://threatpost.com/subtitle-hack-leaves-200-million-vulnerable-to-remote-code-execution/125868/

Opravy zraniteľností pre komponenty Linuxových OS

V máji boli vydané opravy na zraniteľnosti vo viacerých softvérových komponentoch, využívaných v rámci platformy Linux. Za zmienku stojí zraniteľnosť CVE-2017-5461 v knižnici Mozilla Nework Security Services (NSS – implementácia SSL/TLS protokolov od spol. Mozilla), ktorá umožňuje útočníkovi spôsobiť zamedzenie dostupnosti služby, prípadne vykonanie škodlivého kódu, spôsobením zápisu do pamäte mimo povolený rozsah pri vykonávaní niektorých Base64 dekódovacích operácií.

Druhou opravenou zraniteľnosťou, ktorú uvádzame, je CVE-2017-8779 v komponente rpcbind a knižnici libtirpc, pri ktorej môže útočník poslaním špeciálne pripraveného XDR paketu na port UDP 111 spôsobiť alokovanie pamäte a jej následné neuvoľnenie (tzv. rpcbomb). Na túto zraniteľnosť je exploit verejne dostupný. Rpcbind je serverová služba priraďujúca univerzálne adresy procesom na serveri, komunikujúcich s klientom cez Remote Procedure Call – protokol umožňujúci vykonať inštrukcie na vzdialenom serveri.

Zraniteľné systémy:
CVE-2017-5461:
NSS 3.21.3 a staršie
NSS 3.22.x až 3.28.3
NSS 3.29.x až 3.29.4
NSS 3.30.0

CVE-2017-8779:
rpcbind 0.2.3.-0.5 a staršie
libtirpc 0.2.5-1.1 a staršie

Odporúčania:
Na väčšine distribúcií by sa v závislosti od používateľských nastavení mali aktualizácie ponúknuť automaticky.

Zdroje:
https://nvd.nist.gov/vuln/detail/CVE-2017-5461
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8779