Mesačný prehľad kritických zraniteľností

Jún 2017

1. Operačné systémy Microsoft Windows

V júni vydala spoločnosť Microsoft opravy viacerých kritických a zero-day zraniteľností. Vydali opravu kritickej zraniteľnosti CVE-2017-8558 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, pričom zraniteľná je len 32-bitová verzia Microsoft Malware Protection Engine.

Ďalšia vydaná oprava sa týka zero-day zraniteľnosti CVE-2017-8543 vo Windows Search Service pri správe objektov v pamäti umožňuje útočníkovi zaslaním špeciálne pripraveného paketu vykonať na diaľku škodlivý kód a prebrať plnú kontrolu nad zariadením. Útok je možný napríklad cez protokol SMB bez akejkoľvek autentifikácie. Zneužívanie tejto zraniteľnosti už bolo zaznamenané.

Bola opravená zero-day zraniteľnosť CVE-2017-8464, ktorá spočíva v spôsobe, akým Windows narába s LNK súbormi. Útočník môže používateľovi podstrčiť prenosné pamäťové zariadenie alebo zdieľané úložisko so špeciálne pripraveným LNK súborom a príslušným škodlivým binárnym súborom. Ak používateľ otvorí dané zariadenie alebo úložisko napríklad vo Windows Explorer, po spracovaní ikony škodlivého LNK súboru sa vykoná aj škodlivý kód z binárneho súboru s právomocami práve prihláseného používateľa. Zneužívanie tejto zraniteľnosti už bolo zaznamenané.

Spoločnosť Microsoft vydala opravy ďalších dvoch kritických zraniteľností CVE-2017-0283 a CVE-2017-8528 vo Windows Uniscribe (sada knižníc pre typografiu), ktoré obe spočívajú v spôsobe narábania s objektami v pamäti. Útočník môže nalákať používateľa navštíviť webstránku so škodlivým obsahom alebo otvoriť škodlivú prílohu v komunikácii, pričom stačí aj otvorenie v paneli náhľadu. Úspešným zneužitím by útočník získal možnosť na diaľku vykonať škodlivý kód a prevziať kontrolu nad zariadením s právomocami práve prihláseného používateľa. Na prvú menovanú zraniteľnosť je exploit verejne dostupný.

Pre komponent Windows Uniscribe bolo v rámci júnového balíka aktualizácií vydaných niekoľko opráv zraniteľností, označených ako dôležité, pričom pre tri z nich sú verejne dostupné exploity. Konkrétne ide o zraniteľnosti CVE-2017-0282, CVE-2017-0284 a CVE-2017-0285. Všetky tieto zraniteľnosti umožňujú útočníkovi spôsobiť únik informácií z pamäte spôsobením čítania pamäte mimo pridelený rozsah. Pre úspešné zneužitie týchto zraniteľností musí útočník nalákať používateľa otvoriť špeciálne pripravený dokument alebo navštíviť stránku s pripraveným škodlivým obsahom.

Tiež bola vydaná oprava kritickej zraniteľnosti CVE-2017-8527 vo Windows knižnici písiem (font library), ktorá umožňuje útočníkovi zneužiť chybu v spôsobe spracovania vložených písiem. Útočník môže pripraviť webovú stránku so škodlivým obsahom alebo vytvoriť špeciálne pripravený súbor a potom nalákať používateľa navštíviť stránku alebo otvoriť súbor v podobe prílohy v elektronickej komunikácii. Úspešným zneužitím by útočník získal možnosť vzdialeného vykonania škodlivého kódu a prebratia kontroly nad zariadením s právomocami práve prihláseného používateľa.

V rámci júnového balíka aktualizácií bola vydaná aj oprava kritickej zraniteľnosti CVE-2017-0294, ktorá útočníkovi umožňuje na diaľku vykonať škodlivý kód zneužitím chyby pri spracovaní CAB súborov. Útočník môže používateľovi podstrčiť špeciálne pripravený CAB súbor, alebo vytvoriť falošný ovládač na sieťovú tlačiareň a ten rovnako posunúť používateľovi na inštaláciu.

Ďalšie vydané opravy sa týkajú kritických zraniteľností CVE-2017-0291 a CVE-2017-0292, ktoré útočníkovi umožňujú zneužitím chyby v spracovaní špeciálne pripraveného PDF súboru vykonať na diaľku škodlivý kód s právomocami práve prihláseného používateľa po tom, ako používateľ tento súbor otvorí.

V rámci júnového balíka aktualizácií boli vydané aj opravy zraniteľností CVE-2017-0286 až CVE-2017-0289 v komponente Windows Graphics Device Interface, pri ktorých môže útočník zneužiť chybu pri narábaní s objektami v pamäti a zapríčiniť uník informácií čítaním mimo pridelený rozsah pamäte. Pre úspešné zneužitie musí používateľ otvoriť špeciálne vytvorený dokument alebo navštíviť webovú stránku so škodlivým obsahom.

V mesiaci júni boli vydané opravy viacerých zraniteľností v kerneli operačného systému Windows, označených ako dôležité, ktoré autentifikovanému útočníkovi umožňovali spustením špeciálne pripravenej aplikácie spôsobiť únik informácií čítaním pamäte mimo pridelený rozsah. Až na dvadsaťtri z týchto zraniteľností sú verejne dostupné exploity. Konkrétne ide o zraniteľnosti CVE-2017-0299, CVE-2017-0300, CVE-2017-8462, CVE-2017-8469 až CVE-2017-8473, CVE-2017-8476 až CVE-2017-8485, CVE-2017-8487 až CVE-2017-8490 a CVE-2017-8492.

Spoločnosť Microsoft v mesiaci júni, kvôli vysokému stupňu ohrozenia, opäť mimoriadne vydala balík aktualizácií pre nepodporované operačné systémy Windows XP, Windows Server 2003 (aj R2), Windows Vista a Windows 8. Tieto aktualizácie je potrebné stiahnuť a nainštalovať ručne. Odkazy na stiahnutie možno nájsť na poslednom odkaze v zozname zdrojov.

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 1.1.13804.0 a starších, ako súčasť softvérov:

- Microsoft Security Essentials
- Microsoft Endpoint Protection
- Microsoft Forefront Endpoint Protection
- Microsoft Forefront Endpoint Protection 2010
- Windows Defender for Windows 7 SP1 32-bit
- Windows Defender for Windows 8.1 for 32-bit systems
- Windows Defender for Windows 10 for 32-bit systems
- Windows Defender for Windows 10 1511 for 32-bit systems
- Windows Defender for Windows 10 1607 for 32-bit systems
- Windows Defender for Windows 10 1703 for 32-bit systems
- Windows Defender for Windows Server 2008 SP2 32-bit
- Windows Intune Endpoint Protection

Nepodporované systémy, pre ktoré boli vydané aktualizácie:

- Windows XP Professional x64 SP2
- Windows XP SP3
- Windows Server 2003 SP2
- Windows Server 2003 x64 SP2
- Windows Vista SP2
- Windows Vista x64 SP2
- Windows 8 for 32-bit systems
- Windows 8 for x64-based systems

Odporúčania:
Odporúčame preveriť, či na 32-bitových systémoch prebehla automatická aktualizácia Microsoft Malware Protection Engine na verziu 1.1.13903.0 alebo novšiu a v prípade potreby ju spustiť manuálne. Okrem toho, kvôli vysokému stupňu ohrozenia v poslednom období, aktívnemu zneužívaniu niektorých zraniteľností a existencii značného počtu verejne dostupných exploitov, 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. Tiež odporúčame aplikovať aktualizácie pre staršie operačné systémy, ktoré možno stiahnuť z posledného odkazu v zdrojoch, pričom je potrebné ich aplikovať ručne.

Zdroje:
https://blogs.technet.microsoft.com/msrc/2017/06/13/june-2017-security-update-release/
https://technet.microsoft.com/en-us/library/security/4025685
https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8543
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8464
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8558
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0283
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8528
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0282
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8527
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0294
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0291
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0292
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0299
https://support.microsoft.com/en-us/help/4025687/microsoft-security-advisory-4025685-guidance-for-older-platforms

2. Kancelárske balíky Microsoft Office a Office Web Apps

V rámci júnového balíka aktualizácií spoločnosť Microsoft vydala v predošlej kapitole spomenuté opravy kritických zraniteľností CVE-2017-0283 a CVE-2017-8528 vo Windows Uniscribe a CVE-2017-8528 v knižnici písiem, ktoré sa týkajú aj aplikácií zo sady Microsoft Office, ako jedného z možných vektorov útoku. Bližší popis zraniteľností je uvedený v predošlej kapitole.

Zraniteľné systémy:
Microsoft Live Meeting 2007 Add-in
Microsoft Live Meeting 2007 Console
Microsoft Lync 2010 (32-bit)
Microsoft Lync 2010 (64-bit)
Microsoft Lync 2010 Attendee
Microsoft Lync 2013 Service Pack 1 (32-bit)
Microsoft Lync 2013 Service Pack 1 (64-bit)
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 Word Viewer
Skype for Business 2016 (32-bit)
Skype for Business 2016 (64-bit)

Odporúčania:
Aplikovať balíky aktualizácií, publikované prostredníctvom služby 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-2017-0283
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8527
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8528

3. Internetové prehliadače

Microsoft Internet Explorer

V rámci júnového balíka aktualizácií boli spoločnosťou Microsoft vydané opravy kritických zraniteľnostií CVE-2017-8517, CVE-2017-8522 a CVE-2017-8524 v JavaScript engine pre IE11, ktoré útočníkovi umožňujú na diaľku vykonať škodlivý kód s právomocami práve prihláseného používateľa. Zraniteľnosť spočíva v chybe pri prístupe ku objektom v pamäti, zneužitie čoho má za následok narušenie integrity pamäte. Na zneužitie zraniteľnosti musí používateľ navštíviť špeciálne vytvorenú webovú stránku so škodlivým obsahom alebo otvorením škodlivého súboru s vloženým JavaScript-om.

Zraniteľné systémy:
Microsoft Internet Explorer 11

Odporúčania:
Odporúčame používateľom a správcom 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-2017-8517
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8522
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8524

Microsoft Edge

Júnový balík aktualizácií pre Microsoft Edge ošetruje kritické zraniteľnosti CVE-2017-8496 a CVE-2017-8497, umožňujúcu útočníkovi spôsobiť narušenie integrity pamäte zneužitím chyby v narábaní s objektami v pamäti. Zneužitie týchto zraniteľností útočníkovi umožní na diaľku vykonať škodlivý kód s právomocami daného používateľa. Pre úspešné zneužitie musí používateľ navštíviť špeciálne pripravenú stránku, prípadne inú stránku s umiestneným škodlivým obsahom alebo otvoriť škodlivú prílohu v elektronickej komunikácii. Pre prvú menovanú zraniteľnosť je verejne dostupný exploit.

Okrem už spomenutých opráv boli tiež vydané pre prehliadač Edge opravy na ďalších sedem kritických zraniteľností: CVE-2017-8499, CVE-2017-8517, CVE-2017-8520, CVE-2017-8522, CVE-2017-8524, CVE-2017-8548 a CVE-2017-8549, z ktorých všetky umožňujú útočníkovi vzdialené vykonanie škodlivého kódu s právomocami práve prihláseného používateľa. Zraniteľnosti spočívajú v chybách pri narábaní s objektami v pamäti v skriptovacom engine JavaScript. Pre úspešné zneužitie musí používateľ navštíviť špeciálne pripravenú webstránku alebo otvoriť škodlivý súbor s vloženým JavaScript-om.

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

Odporúčania:
Vzhľadom na výskyt verejne dostupného exploitu na jednu z uvedených zraniteľností a pravdepodobnosť výskytu ďalších exploitov, odporúčame používateľom a správcom čo najskôr 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-2017-8496
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8497
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8499
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8520

Mozilla Firefox

Spoločnosť Mozilla v júni vydala opravu kritických zraniteľností CVE-2017-5470 a CVE-2017-5471. Zraniteľnosti spočívajú vo väčšom počte chýb v dodržiavaní bezpečného narábania s pamäťou, ktoré útočníkovi umožňujú spôsobiť narušenie integrity pamäte a vysoko pravdepodobne aj vykonať škodlivý kód.

Ďalšia opravená kritická zraniteľnosť, CVE-2017-5472, v komponente FrameLoader umožňuje spôsobiť potenciálne ďalej zneužiteľné zrútenie aplikácie zneužitím chyby v správe pamäte (využitím uvoľnenej pamäte). Ku zneužitiu dochádza počas opätovného generovania CSS rozloženia po tom, ako používateľ navštívil špeciálne vytvorenú webstránku.

Zraniteľné systémy:

Mozilla Firefox ESR 52.1.2 a staršie
Mozilla Firefox 53.0.3 a staršie

Odporúčania:

Odporúčame aktualizovať prehliadač Mozilla Firefox na verzie 54.0 a ESR 52.2.0 alebo novšie. Prehliadač Firefox ponúka aktualizácie automaticky po ich zverejnení. Ak sa tak nestalo, aktualizáciu je možné spustiť manuálne otvorením Menu > Pomocník > O prehliadači Firefox. Kontrola aktualizácie sa spustí súčasne so zobrazením okna s informáciami o aktuálnej verzii.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/mfsa2017-15/
https://www.mozilla.org/en-US/security/advisories/mfsa2017-16/

Google Chrome

Spoločnosť Google vydala v priebehu júna štyri aktualizácie pre prehliadač Chrome, z ktorých dve obsahovali aj opravy zraniteľností. Kritická zraniteľnosť CVE-2017-5070 v komponente V8 (open-source JavaScript engine) spočíva v chybe pri kontrole typu premennej, čo je potenciálne zneužiteľné na vykonanie škodlivého kódu. Rovnako kritické zraniteľnosti CVE-2017-5071 a CVE-2017-5088, spočívajúce v chybnom narábaní s pamäťou, môžu byť útočníkmi zneužité na spôsobenie zrútenia aplikácie.

V rámci júnových aktualizácií bola pre prehliadač Chrome vydaná oprava kritickej zraniteľnosti CVE-2017-5072 v komponente OmniBox (adresový riadok a vyhľadávač), ktorá útočníkovi umožňuje imitovať adresu stránky (address spoofing).

Kritická zraniteľnosť CVE-2017-5073 v náhľade tlače, opravená v rámci júnových aktualizácií, spočíva v chybe v narábaní s pamäťou, konkrétne v pokuse použiť už predtým uvoľnenú pamäť, čo by útočníkovi pravdepodobne mohlo umožniť vykonať na diaľku škodlivý kód.

V júni bola tiež opravená kritická zraniteľnosť CVE-2017-5074 v komponente Apps Bluetooth, spočívajúca v chybe v narábaní s pamäťou. Útočník by mohol pokus o použitie predtým uvoľnenej pamäte potenciálne zneužiť na vykonanie škodlivého kódu.

Poslednou kritickou zraniteľnosťou opravenou v rámci júnový aktualizácií je CVE-2017-5087. Ide o chybu v komponente IndexedDB, ktorá vzdialenému útočníkovi umožňuje uniknúť zo sandbox-u prehliadača Chrome a na diaľku vykonať škodlivý kód, prípadne pokračovať ďalej v útoku.

Zraniteľné systémy:

Google Chrome 59.0.3071.86 a staršie

Odporúčania:

Odporúčame overiť, či sa prehliadač Chrome automaticky aktualizoval na najnovšiu verziu 59.0.3071.115, prípadne novšiu. V prípade potreby odporúčame aplikovať aktualizáciu ručne cez menu otvorením okna s aktuálne nainštalovanou verziou, čo zároveň spustí aj kontrolu dostupnosti aktualizácie.

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 v júni opravu kritických zraniteľností CVE-2017-3075, CVE-2017-3081, CVE-2017-3083 a CVE-2017-3084, ktoré útočníkovi umožňujú na diaľku vykonať škodlivý kód zneužitím chýb v narábaní s pamäťou, konkrétne pokusu použiť predtým uvoľnenú pamäť. Kvôli prehľadnosti uvádzame zraniteľné komponenty v tabuľke:

CVE-2017-3075	ActionScript2 trieda XML
CVE-2017-3081	Chyba pri narábaní s maskami grafických objektov
CVE-2017-3083	Primetime SDK, chyba pri práci s metadátami
CVE-2017-3084	Chyba pri práci s reklamnými metadátami

Ďalšími kritickými zraniteľnosťami, opravenými v rámci júnovej aktualizácie, sú CVE-2017-3076, CVE-2017-3077, CVE-2017-3078, CVE-2017-3079 a CVE-2017-3082. Zneužitím týchto zraniteľností môže útočník spôsobiť narušenie integrity pamäte a získať možnosť vykonať na diaľku škodlivý kód, pričom na prvé tri uvedené zraniteľnosti sú verejne dostupné exploity. Kvôli prehľadnosti uvádzame konkrétne zraniteľné komponenty v podobe tabuľky:

CVE-2017-3076	MPEG-4 AVC
CVE-2017-3077	Parser PNG obrázkov
CVE-2017-3078	Modul ATF (Adobe Texture Format)
CVE-2017-3079	Vnútorná chyba pri reprezentácii rastrových dát
CVE-2017-3082	Trieda LocaleID

Zraniteľné systémy:
Adobe Flash Player 25.0.0.171 a staršie

Odporúčania:
Vzhľadom na verejne dostupné exploity na viaceré z uvedených zraniteľností odporúčame čo najskôr aktualizovať Flash Player na verziu 26.0.0.126 pre prehliadač Google Chrome. Pre prehliadače Microsoft Edge a Microsoft Internet Explorer 11 je aktuálna verzia 26.0.0.120. V závislosti od nastavení používateľa sa aktualizácia udeje automaticky alebo zobrazením dialógového okna s upozornením.

Zdroje:
https://helpx.adobe.com/security/products/flash-player/apsb17-17.html

5. Frameworky

Microsoft .NET

Spoločnosť Microsoft v júni nevydala pre .NET Framework žiadne opravy zraniteľností.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance

Oracle Java

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

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

6. Iné závažné zraniteľnosti

Rozsiahla vlna útokov ransomware

Koncom júna bola zaznamenaná vlna útokov ransomware známeho pod názvami Petya, Nyetya, NotPetya alebo ExPetr. Malvér na svoje šírenie zneužíva zraniteľnosti CVE-2017-0144 a CVE-2017-0145 v protokole SMBv1, známe aj podľa názvu ich exploitu – EternalBlue. Opravy na obe zraniteľnosti boli spoločnosťou Microsoft vydané v rámci marcového bulletinu MS17-010 a mimoriadne boli vydané aj aktualizácie pre nepodporované operačné systémy. Malvér sa po preniknutí na zariadenie pokúsi ďalej šíriť po lokálnej sieti, pričom sa snaží kradnúť prihlasovacie údaje pre ďalšie šírenie a tiež zašifrovať NTFS oddiel na disku vrátane

boot sektora. CSIRT.SK dňa 28.7. vydal varovanie, v ktorom je možné nájsť ďalšie podrobnosti a odporúčané opatrenia na prevenciu útoku a aj po napadnutí (odkaz nižšie).

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 schopnosť malvéru úplne vyradiť z prevádzky celú infraštruktúru, dôrazne odporúčame aplikovať aktualizácie z Microsoft Security Bulletinu MS17-010 (druhý odkaz) a v prípade potreby aj spomenuté aktualizácie pre staršie systémy – potrebné aplikovať ručne (tretí odkaz). Odporúčame používať aktualizovaný antivírusový softvér. Taktiež odporúčame, pokiaľ je to možné, deaktivovať protokol SMBv1 a WMIC. Správcom odporúčame na každom zariadení s operačným systémom Windows vytvoriť súbory „C:\Windows\perfc.dat“ a „C:\Windows\perfc" a nastaviť im povolenia iba na čítanie. Aktivuje sa tým v doteraz známych variantoch malvéru zabudovaný kill-switch, vďaka čomu nedôjde k infikovaniu zariadenia. Ďalšie odporúčania a informácie možno nájsť vo varovaní CSIRT.SK na prvom odkaze.

Zdroje:

https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=155
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

RCE zraniteľnosť v softvéri Skype

V júni bola spoločnosťou Microsoft vydaná oprava zero-day zraniteľnosti CVE-2017-9948 v komunikačnom softvéri Skype, ktorá útočníkovi umožňuje vykonať na diaľku škodlivý kód spôsobením pretečenia zásobníka v pamäti. Pre úspešné zneužitie musí byť útočník aj obeť skontaktovaná cez službu Skype. Útočník sa pripojí cez protokol RDP ku tretiemu systému s aktivovaným zdieľaním schránky (clipboard). Po vytvorení napríklad snímky obrazovky na treťom systéme a následnom nakopírovaní obsahu schránky do Skype komunikácie dôjde ku zrúteniu aplikácie a spomenutému pretečeniu zásobníka na zariadení útočníka aj obete, pričom útočník má vzápätí možnosť dopraviť na zariadenie obete škodlivý kód. Od obete nie je potrebná žiadna interakcia.

Zraniteľné systémy:

Microsoft Skype 7.2

Microsoft Skype 7.35.0.103 a staršie
Microsoft Skype 7.36.0.150 a staršie

Odporúčania:

Vzhľadom na rozšírenosť softvéru Skype a verejne dostupný dôkaz funkčnosti, dôrazne odporúčame overiť, či sa Skype automaticky aktualizoval aspoň na opravenú verziu 7.37.0.103. Koncom júna bola spoločnosťou Microsoft vydaná ďalšia aktualizácia Skype na verziu 7.38.0.101. V prípade, že automatická aktualizácia neprebehla, odporúčame spustiť aktualizáciu ručne cez menu v hornej lište.

Zdroje:

https://www.vulnerability-db.com/?q=articles/2017/05/28/stack-buffer-overflow-zero-day-vulnerability-uncovered-microsoft-skype-v72-v735
https://www.vulnerability-lab.com/get_content.php?id=2071

Viacero kritických zraniteľností v softvéri OpenVPN

V júni bola vydaná aktualizácia pre open-source softvér na vytváranie virtuálnych privátnych sietí OpenVPN, ktorá obsahovala opravy viacerých kritických zraniteľností. Najzávažnejšou zraniteľnosťou je CVE-2017-7521, ktorá spočíva v chybe pri spracovaní SSL certifikátu. Útočník môže špeciálne pripraveným falošným certifikátom spôsobiť viacnásobné uvoľnenie pamäte a následne na diaľku vykonať škodlivý kód na serveri spracúvajúcom podstrčený SSL certifikát.

Druhou opravenou kritickou zraniteľnosťou je CVE-2017-7520, ktorá formou útoku man-in-the-middle medzi používateľom a proxy serverom umožňuje útočníkovi na diaľku ukradnúť používateľovi prihlasovacie údaje na daný server alebo spôsobiť zrútenie klientskej aplikácie OpenVPN na používateľovom zariadení. Zraniteľnosť je možné zneužiť v prípade, že sa používateľ na proxy server autentifikuje pomocou NTLMv2.

Ďalšími kritickými zraniteľnosťami, opravenými v júnovej aktualizácii OpenVPN, sú CVE-2017-7508 a CVE-2017-7522, ktoré obe môžu byť zneužité na zamedzenie dostupnosti serverovej služby OpenVPN. Na zneužitie prvej menovanej zraniteľnosti stačí útočníkovi zaslať na server špeciálne pripravený IPv6 paket. Druhá uvedená zraniteľnosť spočíva v chybe pri spracovaní klientskeho certifikátu, kvôli chybe pri narábaní s objektom v pamäti.

Zraniteľné systémy:

OpenVPN verzie 2.4.2 a staršej
OpenVPN verzie 2.3.16 a staršej

Odporúčania:

Vzhľadom na verejne dostupné detaily ohľadom uvedených zraniteľností, odporúčame čo najskôr aktualizovať softvér OpenVPN na verziu 2.4.3 alebo v prípade potreby na 2.3.17. Aktualizované verzie možno stiahnuť na druhom z odkazov uvedených nižšie.

Zdroje:

https://guidovranken.wordpress.com/2017/06/21/the-openvpn-post-audit-bug-bonanza/
https://openvpn.net/index.php/open-source/downloads.html

Zraniteľnosti v komponente Systemd operačných systémov Linux

V mesiaci júni bola vydaná pre operačné systémy Ubuntu a ich deriváty aktualizácia spúšťacieho démona a správcu služieb Systemd. Kritická zraniteľnosť CVE-2017-9445 v komponente systemd-resolve umožňuje útočníkovi vytvoriť škodlivý DNS server, ktorý na používateľove zariadenie odošle špeciálne vytvorený DNS paket. To spôsobí zápis mimo pridelenú pamäť, čo môže útočník zneužiť na vykonanie škodlivého kódu, alebo zamedzenie dostupnosti služby.

V júni bola nahlásená aj ďalšia potenciálna zraniteľnosť v Systemd, v čase písania tohto prehľadu bez prideleného CVE kódu. Zraniteľnosť umožňuje lokálnemu a potenciálne aj vzdialenému útočníkovi dosiahnuť povýšenie oprávnení zneužitím spôsobu, akým Systemd spracúva konfiguračné skripty. V prípade, že používateľské meno používateľa aj so základnými právomocami začína číslicou, Systemd o tomto podá správu do logu, avšak pokračuje v spúšťaní služby, ktorú spustí s právomocami root. Treba poznamenať, že používateľské meno začínajúce číslicou je nesprávne.

Zraniteľné systémy:

Ubuntu 16.10 so Systemd verzie 231-9git1 a staršej
Ubuntu 17.04 so Systemd verzie 232-21ubuntu2 a staršej

Deriváty Ubuntu

Odporúčania:

Odporúčame aplikovať aktualizácie distribuované cez repozitáre a aplikovateľné pomocou správcu balíkov. V prípade druhej menovanej zraniteľnosti odporúčame pri vytváraní používateľského mena vyžadovať, aby nezačínalo číslicou, aj napriek tomu, že by na danej distribúcii bolo možné takéhoto používateľa vytvoriť.

Zdroje:

https://www.ubuntu.com/usn/usn-3341-1/
https://github.com/systemd/systemd/issues/6237

Zraniteľnosť vo VMWare vSphere Data Protection

V júni bola spoločnosťou VMWare vydaná aktualizácia pre softvér vSphere Data Protection (zálohovanie a správu záloh virtuálnych zariadení), v rámci ktorej boli opravené dve kritické zraniteľnosti. Prvou z nich je zraniteľnosť CVE-2017-4914, ktorá umožňuje útočníkovi na diaľku zneužiť chybu pri deserializácii zaslaním špeciálne vytvoreného paketu a následne prebrať kontrolu nad cieľovým zariadením a vykonať na diaľku škodlivý kód. Na túto zraniteľnosť je exploit verejne dostupný.

Druhou opravenou kritickou zraniteľnosťou v softvéri Vsphere Data Protection je zraniteľnosť CVE-2017-4917, spočívajúca v prelomiteľnom šifrovaní prihlasovacích údajov do aplikácie vCenter Server (správa virtuálnych systémov a zariadení), ktorá útočníkovi umožňuje získať tieto prihlasovacie údaje v obyčajnom textovom formáte.

Zraniteľné systémy:

VMWare vSphere Data Protection 6.1.3 a staršie
VMWare vSphere Data Protection 6.0.4 a staršie
VMWare vSphere Data Protection 5.8.4 a staršie
VMWare vSphere Data Protection 5.5.7 a staršie

Odporúčania:

Vzhľadom na závažnosť zraniteľností a existenciu verejne dostupného exploitu, odporúčame čo najskôr aktualizovať softvér vSphere Data Protection na opravenú verziu 6.1.4 alebo v prípade potreby na opravenú verziu 6.0.5.

Zdroje:

https://www.vmware.com/security/advisories/VMSA-2017-0010.html
https://www.vmware.com/security/advisories/VMSA-2017-0010.html