Mesačný prehľad kritických zraniteľností

Január 2018

1. Operačné systémy Microsoft Windows

V mesiaci január nevydala spoločnosť Microsoft žiadne opravy kritických zraniteľností v operačných systémoch Windows. Vydala však niekoľko opráv dôležitých zraniteľností, pre ktoré existujú verejne dostupné exploity. Na zneužitie týchto zraniteľností sa útočník musí prihlásiť do systému a spustiť špeciálne navrhnutú aplikáciu.

Dôležitú zraniteľnosť CVE-2018-0743 charakterizuje neautorizované získanie väčších oprávnení spôsobené pretečením premennej typu integer v komponente Windows Subsystem for Linux. Úspešné zneužitie umožní útočníkovi spúšťať kód s povýšenými právomocami.

Podobne zraniteľnosť CVE-2018-0744 môže byť zneužitá na neautorizované povýšenie oprávnení pri tom, ako Windows Kernel chybne narába s objektmi v pamäti. Úspešné zneužitie dáva možnosť spustiť ľubovoľný kód v Kernel móde, útočník môže potom inštalovať program, prezerať, meniť a mazať dáta, vytvárať nové užívateľské účty s používateľskými právami.

CVE-2018-0745 a CVE-2018-0746 sú zraniteľnosti vo Windows Kernel umožňujúce získať informáciu vedúcu k obídeniu Kernel Address Space Layout Randomization. Úspešné zneužitie umožní útočníkovi získať adresu objektu jadra v pamäti.

Zraniteľnosti CVE-2018-0748, CVE-2018-0751, CVE-2018-0752 umožňujú neautorizované získanie väčších oprávnení. To nastáva pri spôsobe, akým Windows Kernel API spravuje povolenia. Úspešné zneužitie dáva útočníkovi možnosť zosobniť procesy, vkladať komunikáciu medzi procesmi, či narušiť funkčnosť systému.

Napokon zraniteľnosť CVE-2018-0749 umožňuje neautorizované získanie väčších oprávnení zneužitím zraniteľnosti v Microsoft Server Message Block (SMB) Server. Uplatní sa, keď sa útočník s platnými prihlasovacími údajmi pokúsi otvoriť špeciálne navrhnutý súbor cez SMB protokol na tom istom počítači. Úspešné zneužitie dáva útočníkovi možnosť obísť určité bezpečnostné kontroly v operačnom systéme.

Zraniteľné systémy:

Microsoft Windows Server 2016
Microsoft Windows Server 2016 (Server Core Installation)
Microsoft Windows Server 2012 R2
Microsoft Windows Server 2012 R2 (Server Core Installation)
Microsoft Windows Server 2012
Microsoft Windows Server 2012 (Server Core Installation)
Microsoft Windows Server version 1709 (Server Core Installation)
Microsoft Windows RT 8.1
Microsoft Windows 8.1 for x64-based Systems
Microsoft Windows 8.1 for 32-bit Systems
Microsoft Windows Server 2008 R2 for x64-based Systems SP1
Microsoft Windows Server 2008 R2 for x64-based Systems SP1 (Server Core Installation)
Microsoft Windows Server 2008 R2 for Itanium-based Systems SP1
Microsoft Windows Server 2008 for x64-based Systems SP2
Microsoft Windows Server 2008 for x64-based Systems SP2 (Server Core Installation)
Microsoft Windows Server 2008 for Itanium-based Systems SP2
Microsoft Windows Server 2008 for 32-bit Systems SP2
Microsoft Windows Server 2008 for 32-bit Systems SP2 (Server Core Installation)
Microsoft Windows 7 for x64-based Systems SP1
Microsoft Windows 7 for 32-bit Systems SP1
Microsoft Windows 10 version 1709 for x64-based Systems
Microsoft Windows 10 version 1709 for 32-bit Systems
Microsoft Windows 10 version 1703 for x64-based Systems
Microsoft Windows 10 version 1703 for 32-bit Systems
Microsoft Windows 10 Version 1607 for x64-based Systems

Microsoft Windows 10 Version 1607 for 32-bit Systems
Microsoft Windows 10 version 1511 for x64-based Systems
Microsoft Windows 10 version 1511 for 32-bit Systems
Microsoft Windows 10 for x64-based Systems
Microsoft Windows 10 for 32-bit Systems

Odporúčania:

Vzhľadom na to, že k uvedeným zraniteľnostiam existujú verejne dostupné exploity, odporúčame bezodkladne aplikovať aktualizácie, 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-2018-0743
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0744
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0745
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0748
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0749

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft vydala v mesiaci január opravu jednej kritickej zraniteľnosti. Zraniteľnosť CVE-2018-0797 umožňuje vzdialené vykonanie kódu spôsobené nesprávnym narábaním s RTF súbormi. Pre jej zneužitie musí užívateľ otvoriť špeciálne navrhnutý súbor. Tento môže útočník doručiť napríklad e-mailom, alebo cez vlastnú či kompromitovanú webstránku. Útočník musí používateľa presvedčiť, aby súbor spustil. Úspešné zneužitie dáva útočníkovi možnosť spustiť ľubovoľný kód s právomocami aktuálneho používateľa. Ak má prihlásený užívateľ administrátorské právomoci, útočník môže prevziať kontrolu nad systémom, inštalovať programy, prezerať, meniť a mazať dáta, či vytvárať nové užívateľské účty s používateľskými právami.

Zraniteľné systémy:

Microsoft Word 2016 (64-bit edition)
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2013 Service Pack 1 (64-bit editions)
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2010 Service Pack 2 (64-bit editions)
Microsoft Word 2010 Service Pack 2 (32-bit editions)
Microsoft Word 2007 SP3
Microsoft SharePoint Server 2010 SP2
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft Office Word Viewer
Microsoft Office Web Apps Server 2013 SP1
Microsoft Office Web Apps 2010 SP2
Microsoft Office Online Server 2016
Microsoft Office Compatibility Pack Service Pack 3
Microsoft Office 2016 for Mac
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2010 Service Pack 2 (32-bit editions)

Odporúčania:

Vzhľadom na závažnosť uvedenej zraniteľnosti odporúčame bezodkladne aplikovať aktualizácie 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-2018-0797

3. Internetové prehliadače

Microsoft Internet Explorer

V rámci januárového balíka opráv boli spoločnosťou Microsoft vydané opravy dvoch kritických zraniteľností.

Zraniteľnosti CVE-2018-0762 a CVE-2018-0772 umožňujú vzdialené vykonanie kódu. Spočívajú v spôsobe, akým skriptovací engine narába s objektmi v pamäti a možno ich zneužiť na narušenie integrity pamäte spôsobom, ktorý umožní útočníkovi spúšťať ľubovoľný kód s právomocami aktuálneho používateľa. Útočník môže presvedčiť používateľa, aby navštívil jeho špeciálne vytvorenú webstránku, navrhnutú na zneužitie zraniteľnosti. Útočník môže tiež vložiť ovládací prvok ActiveX označený „Bezpečné na inicializáciu“ do aplikácie, alebo MS Office dokumentu. Útočník môže svoj nástroj umiestniť aj na kompromitovanú webstránku, alebo webstránku s užívateľským obsahom či reklamou. Úspešné zneužitie dáva útočníkovi možnosť získať právomoci aktuálneho používateľa. Ak má prihlásený užívateľ administrátorské právomoci, útočník môže prevziať kontrolu nad systémom, inštalovať programy, prezerať, meniť a mazať dáta, či vytvárať nové užívateľské účty s používateľskými právami.

Zraniteľné systémy:

Microsoft Internet Explorer 11

Odporúčania:

Vzhľadom na závažnosť popisovaných zraniteľností odporúčame čo najskôr aplikovať aktualizácie, 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-2018-0762

Microsoft Edge

V rámci januárového balíka aktualizácií boli vydané opravy troch skupín kritických zraniteľností.

Zraniteľnosti CVE-2018-0758, CVE-2018-0769, CVE-2018-0770, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778 a CVE-2018-0781 spočívajú v spôsobe, akým skriptovací engine narába s objektmi v pamäti, pričom ich zneužitím možno zapríčiniť narušenie integrity pamäte spôsobom, ktorý umožní útočníkovi spúšťať ľubovoľný kód s právomocami aktuálneho používateľa. Zneužiť ich útočník môže tak, že presvedčí používateľa, aby navštívil jeho špeciálne vytvorenú webstránku, navrhnutú na zneužitie zraniteľnosti cez internetový prehliadač Edge. Útočník môže umiestniť špeciálny obsah určený na zneužitie zraniteľnosti aj na kompromitovanú webstránku, alebo webstránku s užívateľským obsahom či reklamou. Ak má prihlásený užívateľ administrátorské právomoci, útočník môže prevziať kontrolu nad systémom, inštalovať programy, prezerať, meniť a mazať dáta, či vytvárať nové užívateľské účty s používateľskými právami. Na niektoré z týchto zraniteľností sú dostupné verejné exploity.

Zraniteľnosti CVE-2018-0762 a CVE-2018-0772 spočívajú v spôsobe, akým skriptovací engine narába s objektmi v pamäti, pričom ich zneužitiemôže zapríčiniť narušenie integrity pamäte spôsobom, ktorý umožní útočníkovi spúšťať ľubovoľný kód s právomocami aktuálneho používateľa. Pre bližší popis viď časť Microsoft Internet Explorer, ktorej sa tieto zraniteľnosti tiež dotýkajú.

Kritické zraniteľnosti CVE-2018-0767, CVE-2018-0780 a CVE-2018-0800 umožňujú útočníkovi spôsobiť únik informácií, zneužitím chyby pri narábaní s objektmi v pamäti. Útočník môže tieto zraniteľnosti zneužiť tak, že presvedčí používateľa, aby navštívil jeho špeciálne vytvorenú webstránku. Útočník môže umiestniť špeciálny obsah určený na zneužitie zraniteľnosti aj na kompromitovanú webstránku, alebo webstránku s užívateľským obsahom či reklamou. Získané informácie môže útočník zneužiť na ďalšiu kompromitáciu používateľovho systému. Ku dvom z troch týchto zraniteľností existuje verejne dostupný exploit.

Zraniteľné systémy:

Microsoft Edge v systémoch Windows 10 verzií 1511, 1607, 1703 a 1709 a 32-bitových aj 64-bitových verziách
Microsoft Edge v systéme Windows Server 2016

Odporúčania:

Vzhľadom na závažnosť popisovaných zraniteľností a verejnú dostupnosť exploitov pre niektoré z nich, odporúčame čo najskôr aplikovať aktualizácie, 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-2018-0758
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0762
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0767

Mozilla Firefox

Spoločnosť Mozilla vydala v januári opravu štyroch kritických zraniteľností v prehliadači Firefox.

Zraniteľnosti CVE-2018-5089 a CVE-2018-5090 súvisia s chybami zabezpečenia pamäte. Niektoré z týchto chýb vykazujú znaky narušenia integrity pamäte a mohli by byť zneužité na spustenie ľubovoľného kódu.

Zraniteľnosť CVE-2018-5091 spočíva v opätovnom použití už predtým uvoľnenej pamäte. Môže nastať počas WebRTC pripojení pri interakcii s DTMF časovačmi a spôsobiť potenciálne zneužiteľné zrútenie aplikácie.

Zraniteľnosť CVE-2018-5124 vzniká pri nedostatočnej sanitizácii HTML útržkov v chrome (komponent Firefoxu) privilegovaných dokumentoch. Útočník musí presvedčiť používateľa, aby klikol na špeciálne navrhnutý odkaz, alebo otvoril súbor. Úspešné zneužitie môže poskytnúť útočníkovi možnosť spúšťať ľubovoľný kód s používateľskými oprávneniami.

Zraniteľné systémy:

Mozilla Firefox 58 a staršie
Mozilla Firefox ESR 52.5.3 a staršie

Odporúčania:

Odporúčame aktualizovať prehliadač Mozilla Firefox na verziu 58.0.1, resp. ESR 52.6. 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/mfsa2018-02/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-05/
https://www.helpnetsecurity.com/2018/01/31/cve-2018-5124/

Google Chrome

Spoločnosť Google v januári vydala dve aktualizácie pre prehliadač Chrome.

Aktualizácia zo 4. januára neobsahovala zverejnené informácie o prípadných opravách zraniteľností.

V rámci aktualizácie z 24. januára boli vydané opravy na 53 zraniteľností. Medzi nimi sa nachádzajú tri kritické. Pri CVE-2018-6031 sa jedná o zraniteľnosť pamäte typu použi-po-uvoľnení v komponente PDFium, u CVE-2018-6032 ide o obídenie politiky rovnakého pôvodu (same origin policy) v správe doplnkov prehliadača a pri CVE-2018-6033 nastáva súbeh pri otvorení stiahnutých súborov.

Zraniteľné systémy:

Google Chrome 63.0.3239.132 a staršie

Odporúčania:

Odporúčame overiť, či sa prehliadač Chrome automaticky aktualizoval na verziu 64.0.3282.119, 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/2018/
https://chromereleases.googleblog.com/2018/01/stable-channel-update-for-desktop.html

https://chromereleases.googleblog.com/2018/01/stable-channel-update-for-desktop_24.html

4. Adobe Flash Player

Spoločnosť Adobe nevydala v mesiaci január pre aplikáciu Adobe Flash Player žiadne opravy kritických zraniteľností.

Zdroje:
https://helpx.adobe.com/security.html

5. Frameworky

Microsoft .NET

V rámci januárového balíka aktualizácií spoločnosť Microsoft nevydala žiadne opravy kritických zraniteľností vo frameworkoch .NET. Vydala však tri opravy pre dôležité zraniteľnosti.

Zraniteľnosť CVE-2018-0764 spôsobuje obmedzenie dostupnosti služby (DoS). To nastáva, keď .NET a .NET Core nevhodne spracúva XML dokumenty. Zneužiť je ju možné vzdialene bez autentifikácie, pričom útočník pošle špeciálne zostrojené požiadavky pre .NET / .NET Core aplikáciu. Úspešné zneužitie dáva útočníkovi možnosť spôsobiť obmedzenie dostupnosti služby (DoS) .NET aplikácii.

Neautorizované získanie väčších oprávnení umožňuje zraniteľnosť CVE-2018-0784 pri tom, ako webová aplikácia ASP.NET Core, vytvorená s použitím zraniteľných projektových vzorov, nevhodne ošetrí webové požiadavky. K zneužitiu môže dôjsť tak, že útočník môže poslať e-mailom (prípadne iným spôsobom) užívateľovi špeciálne vytvorený škodlivý odkaz. Ďalej musí užívateľa presvedčiť, aby na odkaz klikol. Úspešné zneužitie dáva možnosť útočníkovi vykonávať útoky injektovaním obsahu a spúšťať skript v kontexte zabezpečenia prihláseného užívateľa.

Zraniteľnosť CVE-2018-0786 sa týka obídenia bezpečnostnej funkcie. Dôjde k tomu v prípade, keď Microsoft .NET Framework a .NET Core komponenty neúplne overia certifikáty. Útočník môže poskytnúť neplatný certifikát na špecifický účel, no daný komponent .NET ho napriek tomu použije.

Zraniteľné systémy:
.NET Core 1.0
.NET Core 1.1
.NET Core 2.0
Microsoft .NET 2.0
Microsoft .NET 3.0
Microsoft .NET 3.5
Microsoft .NET 3.5.1
Microsoft .NET 4.5.2
Microsoft .NET 4.6
Microsoft .NET 4.6.1
Microsoft .NET 4.6.2
Microsoft .NET 4.7
Microsoft .NET 4.7.1
ASP.NET Core 2.0

Odporúčania:
Odporúčame aplikovať aktualizácie 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-2018-0764
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0784
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0786

Oracle Java

Spoločnosť Oracle v mesiaci január vydala balík opráv 21 zraniteľností. 18 z nich môže byť zneužitých na diaľku neautentifikovaným útočníkom. Z nich tri najrizikovejšie sú CVE-2018-2638 (zraniteľnosť komponentu Deployment), CVE-2018-2639 (opäť súvisí s komponentom Deployment) a CVE-2018-2633 (zraniteľnosť komponentu JNDI). Pre úspešné zneužitie týchto zraniteľností je potrebná aj interakcia používateľa.

Zraniteľné systémy:

Java SE: 8u152, 7u161, 6u171, 9.0.1 a staršie
Java SE Embedded: 8u151 a staršie

Odporúčania:

Vzhľadom na závažnosť uvedených zraniteľností odporúčame čo najskôr aktualizovať zraniteľné verzie Java SE a Java SE Embedded na aktuálne verzie, t.j. Java SE
6u181, Java SE 7u171, Java SE 8u161, Java 9.0.4 a Java SE Embedded 8u161, prostredníctvom Java Auto Update, alebo na stránke spoločnosti Oracle, viď spodný odkaz v zdrojoch.

Zdroje:

http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
http://www.oracle.com/technetwork/indexes/downloads/index.html#java

6. Iné závažné zraniteľnosti

Meltdown a Spectre – kritické zraniteľnosti procesorov

O kritických zraniteľnostiach procesorov vyplývajúcich z ich hardvérového prevedenia vydal CSIRT.SK dňa 8.1.2018 varovanie (viď link). Tieto zraniteľnosti súvisia s funkciou speculative execution, ktorú využívajú prakticky všetky procesory vyrábané od roku 1995 na zvýšenie svojho výkonu. Úspešné zneužitie môže dovoliť pristupovať užívateľským aplikáciám ku chráneným dátam v systémovej pamäti (porušenie funkcie Kernel Page Table Isolation).

Zraniteľnosť Meltdown (CVE-2017-5754) spočíva v možnosti prístupu užívateľských aplikácií k celej fyzickej pamäti počítača. Je pomerne dobre softvérovo opraviteľná.

Zraniteľnosť Spectre (CVE-2017-5753, CVE-2017-5715) núti spustený program pristupovať na náhodné miesta v pamäti, pričom postranným kanálom je možné čítať tam zapísané dáta. Zneužitie sa dá realizovať napríklad JavaScript kódom a dokáže prekonať funkciu sandbox internetového prehliadača. Táto zraniteľnosť je ťažšie zneužiteľná, no zároveň sa nedá celkom opraviť softvérovým riešením.

Opravy vydávajú okrem poskytovateľov operačných systémov aj výrobcovia procesorov. Spoločnosť Intel v druhej polovici januára stiahla jednu z verzií svojej opravy s upozornením, aby ju užívatelia neinštalovali. Spôsobovala náhodné reštartovanie systému.

Zraniteľné systémy:

Procesory Intel
Procesory AMD
Procesory ARM

Odporúčania:

Pretože sa jedná o zraniteľnosti podmienené samotným hardvérovým prevedením procesorov, nie je možné ich opraviť úplne. Výrobcovia operačných systémov a iného programového vybavenia však vydali opravy, ktoré odporúčame aplikovať. Spravidla sú súčasťou automatických aktualizácií. Výrobcovia operačných systémov budú na odstraňovaní, resp. zmiernení následkov týchto zraniteľností pracovať aj v budúcnosti.

Zdroje:

https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=157
https://threatpost.com/intel-halts-spectre-meltdown-patching-for-broadwell-and-haswell-systems/129615/

Ďalšia zraniteľnosť procesorov Intel – AMT

V januári bola odhalená ďalšia hardvérová zraniteľnosť. Týka sa technológie Active Management Technology v procesoroch Intel, ktorá umožňuje IT administratívam lepšiu kontrolu a efektívnejšie vzdialené opravy výpočtovej techniky v organizáciách. Zraniteľnosť môže umožniť útočníkovi obísť prihlasovací proces a prevziať kontrolu nad používateľovým počítačom v priebehu 30 sekúnd.

Útočník potrebuje fyzický prístup k systému, pričom sa (aj v prípade zaheslovaného BIOSu) dokáže dostať do rozšírenia Intel Management Engine BIOS Extension (MEBx) a nastaviť konfiguráciu umožňujúcu vzdialené zneužitie systému. K tomu mu stačí použiť predvolené heslo „admin“, ktoré bude pravdepodobne zachované vo väčšine korporátnych zariadení.

Zraniteľné systémy:

Systémy postavené na procesoroch Intel, určených pre organizácie

Odporúčania:

Odporúčame korporátnym klientom zmeniť predvolené heslá do časti BIOSu AMT za silné, alebo vypnúť túto funkciu, ak je to možné. Taktiež je žiadúce nenechávať na verejných miestach zariadenie bez dozoru.

Zdroje:

https://thehackernews.com/2018/01/intel-amt-vulnerability.html
https://threatpost.com/intel-amt-loophole-allows-hackers-to-gain-control-of-some-pcs-in-under-a-minute/129408/

Kritická zraniteľnosť v Electron JS Framework

V januári bola vydaná oprava na kritickú zraniteľnosť CVE-2018-1000006 populárnej platformy Electron na vývoj webových aplikácií, napríklad Skype, Signal, Wordpress a Slack. Zneužitie tejto zraniteľnosti umožňuje útočníkovi vzdialené vykonanie kódu.

Zraniteľné sú Electron aplikácie bežiace pod operačným systémom Windows, ktoré registrujú seba ako predvolený obslužný nástroj niektorého protokolu (ako napr. myapp://). Nezávisí na spôsobe registrácie protokolu – s využitím natívneho kódu, Windows registry, alebo Electron API (app.setAsDefaultProtocolClient).

Zraniteľné systémy:

Electron 1.8.2-beta.3 a staršie
Electron 1.7.10 a staršie
Electron 1.6.15 a staršie

Odporúčania:

Vzhľadom na závažnosť zraniteľností odporúčame bezodkladne aktualizovať Electron na verzie 1.8.2-beta.5, 1.7.12 a 1.6.17. Použiť na to môžete prvý odkaz v zdrojoch. Ak aktualizácia nie je možná, použite „--“ ako posledný argument pri volaní app.setAsDefaultProtocolClient, čím ohlásite koniec príkazových možností.

Zdroje:

https://github.com/electron/electron/releases/
https://electronjs.org/blog/protocol-handler-fix
https://thehackernews.com/2018/01/electron-js-hacking.html

Zraniteľnosť vo VMware vSphere Data Protection

V januári bola spoločnosťou VMware vydaná aktualizácia pre softvér vSphere Data Protection (zálohovanie a správa záloh virtuálnych zariadení), v rámci ktorej boli opravené tri kritické zraniteľnosti. Prvou z nich je zraniteľnosť CVE-2017-15548, ktorá umožňuje útočníkovi na diaľku obísť autentifikáciu v aplikácii a získať neoprávnený prístup k root-u.

Druhou opravenou kritickou zraniteľnosťou je CVE-2017-15549. Spočíva v možnosti autentifikovaného vzdialeného útočníka s nízkymi právomocami nahrávať ľubovoľný škodlivý súbor do ktorejkoľvek lokality v systéme súborov servera.

Tretia zraniteľnosť CVE-2017-15550 umožňuje vzdialenému útočníkovi s nízkymi právomocami pristupovať k ľubovoľným súborom v systéme súborov servera.

Zraniteľné systémy:

VMWare vSphere Data Protection 6.1.x
VMWare vSphere Data Protection 6.0.x
VMWare vSphere Data Protection 5.x

Odporúčania:

Vzhľadom na závažnosť zraniteľností odporúčame čo najskôr aktualizovať softvér vSphere Data Protection na opravenú verziu 6.1.6 alebo v prípade potreby na opravenú verziu 6.0.7.

Zdroje:

https://www.vmware.com/security/advisories/VMSA-2018-0001.html
https://threatpost.com/vmware-issues-3-critical-patches-for-vsphere-data-protection/129277/