Mesačný prehľad kritických zraniteľností
Marec 2018

1. Operačné systémy Microsoft Windows

V marci neboli zaznamenané žiadne kritické zraniteľnosti operačného systému Microsoft Windows. Bolo však opravených viac ako dva tucty závažných zraniteľností. Veľa z nich sa týka nesprávneho narábania s objektmi v pamäti. Útočník môže pomocou špeciálne upravenej aplikácie získať citlivé informácie, ktoré vie ďalej zneužiť. Ostatné zraniteľnosti taktiež umožňujú útočníkovi sa dostať k citlivým informáciám alebo vzdialene spustiť škodlivý kód.

Po aktualizácii, ktorá opravuje zraniteľnosť meltdown sa na Windows 7 x64 a Windows Server 2008 R2 x64 objavila nová zraniteľnosť. Konkrétne ide o CVE-2018-1038, ktorá nastane, keď jadro systému Windows nesprávne narába s objektmi v pamäti. Útočník po úspešnom zneužití tejto zraniteľnosti môže inštalovať programy, čítať, meniť a mazať dáta a taktiež vytvárať plnohodnotné účty.

Zraniteľné systémy:

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 10 Version 1709 for 32-bit Systems
Windows 10 Version 1709 for x64-based Systems
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 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 Itanium-Based Systems Service Pack 2
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 R2 for Itanium-based Systems Service Pack 1
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 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016

Windows Server 2016 (Server Core installation)
Windows Server, version 1709 (Server Core installation)

Odporúčania:

Vzhľadom na množstvo závažných zraniteľností 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-2018-0926
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0899
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0814
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0811
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0813
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1038
https://www.kb.cert.org/vuls/id/277400

2. Kancelárske balíky Microsoft Office a Office Web Apps

Závažné zraniteľnosti CVE-2018-0910 až CVE-2018-0917, CVE-2018-0921, CVE-2018-0944, CVE-2018-8551, CVE-2018-0947 sa týkajú zvýšenia privilégií. Ak útočník pošle špeciálne upravenú požiadavku zasiahnutému serveru služby SharePoint dokáže zneužiť zraniteľnosť tohto typu. Je potom možné vykonávať cross-site scripting útoky a spúšťať skripty ako práve prihlásený používateľ. To môže útočníkovi umožniť čítanie obsahu na ktorý nemá právo, vykonať akcie ako zmenu práv, zmazanie obsahu alebo vloženie škodlivého obsahu na SharePoint stránke v mene používateľa.

V kancelárskom balíku Microsoft Office sa tento mesiac objavila zraniteľnosť CVE-2018-0919, ktorá môže spôsobiť únik citlivých informácií. Kvôli neinicializovanej premennej môže dôjsť k čítaniu pamäte mimo hraníc a môže sa tak stať, že bude odhalený obsah tejto pamäte. Zneužitie je možné iba ak používateľ otvorí špeciálne upravený dokument poškodenou verziou softvéru Microsoft Office.

Okrem tejto zraniteľnosti sa v kancelárskom balíku Microsoft Office objavila ešte jedna závažná zraniteľnosť, konkrétne CVE-2018-0922, ktorá je spôsobená nesprávnym narábaním s objektmi v pamäti. Zneužiť ju je možné len ak používateľ otvorí špeciálne upravený dokument, ktorý sa k nemu môže dostať napríklad pomocou e-mailu alebo cez webstránku.

Zraniteľnosť CVE-2018-0907 Microsoft Office Excelu umožňuje obísť nastavenia vykonávania makier v dokumente. Útočník môže zraniteľnosť zneužiť vložením ovládacieho prvku do hárka programu Excel, ktorým špecifikuje, že by sa malo pustiť makro. Zneužitie tejto zraniteľnosti je možné len za pomoci používateľa, ktorý by musel otvoriť špeciálne upravený súbor.

Zraniteľné systémy:

Microsoft Project Server 2013 Service Pack 1
Microsoft Project Server 2010 Service Pack 2
Microsoft SharePoint Enterprise Server 2016
Microsoft Office Compatibility Pack Service Pack 3
Microsoft Office Word Viewer
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2016 Click-to-run (C2R) for 32-bit editions
Microsoft Office 2016 Click-to-run (C2R) for 64-bit editions
Microsoft Office 2016 for Mac
Microsoft Office Online Server 2016
Microsoft Office Web Apps 2010 Service Pack 2
Microsoft Office Web Apps 2013 Service Pack 1
Microsoft Excel 2010 Service Pack 2 (32-bit editions)
Microsoft Excel 2010 Service Pack 2 (64-bit editions)
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Excel 2007 Service Pack 3

Odporúčania:

Vzhľadom množstvo závažných zraniteľností 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-2018-0910
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0911
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0912
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0913
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0914
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0915
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0916
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0917
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0921
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8551
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0944
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0919

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0922
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0907

3. Internetové prehliadače

Microsoft Internet Explorer

V rámci marcového balíka opráv boli spoločnosťou Microsoft vydané opravy jednej kritickej zraniteľnosti.
Konkrétne má táto zraniteľnosť označenie CVE-2018-0840 a umožňuje útočníkovi získať citlivé informácie. Nesprávne narábanie s objektmi v pamäti môže poskytnúť útočníkovi informácie, ktoré môže ďalej zneužiť. Na úspešné zneužitie tejto zraniteľnosti útočník potrebuje presvedčiť používateľa aby navštívil jeho špeciálne vytvorenú webstránku.

Zraniteľné systémy:

Microsoft Internet Explorer 11 v systémoch Windows 10 verzií 1511,1607, 1703, 1709 v 32 aj 64 bitových verziách
Microsoft Internet Explorer 11 pre systém Windows Server 2012 R2

Odporúčania:

Vzhľadom závažnosť 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-2018-0932

Microsoft Edge

14. marca bola zverejnená aktualizácia, ktorá opravuje viacero kritických zraniteľností umožňujúcich vykonať škodlivý kód na diaľku. Po tejto aktualizácii bol na súťaži pwn2own prezentovaný exploit pomocou chyby použitia už uvoľnenej pamäte.
CVE-2018-0872, CVE-2018-0874, CVE-2018-0876, CVE-2018-0893, CVE-2018-0930, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934 – všetky tieto zraniteľnosti umožňujú útočníkovi spustiť ľubovoľný kód, keďže skriptovací engine nesprávne narába s objektmi v pamäti. Zneužitie je možné len za pomoci používateľa, ktorého musí útočník presvedčiť aby navštívil jeho špeciálne vytvorenú stránku. Úspešné zneužitie týchto zraniteľností umožňuje útočníkovi prebrať kontrolu nad systémom a vykonať ľubovoľný škodlivý kód s oprávneniami práve prihláseného používateľa. V prípade, že používateľ mal administrátorské práva, útočník získa možnosť inštalovať programy, prezerať, meniť a mazať dáta, prípadne vytvárať plnohodnotné používateľské účty.
CVE-2018-0891, CVE-2018-0927, CVE-2018-0932, CVE-2018-0939, CVE-2018-0879 – tieto závažné a kritické zraniteľnosti dávajú útočníkovi prístup k citlivým informáciám v systéme používateľa. Tieto zraniteľnosti je taktiež možné zneužiť len za pomoci používateľa a to podobným spôsobom ako vyššie spomínané zraniteľnosti prehliadača Microsoft Edge.

Zraniteľné systémy:

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

Odporúčania:

Vzhľadom na závažnosť a množstvo uvedených zraniteľností 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-2018-0872
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0874
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0876
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0893
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0930
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0931
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0932
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0933
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0934

Mozilla Firefox

Spoločnosť Mozilla v mesiaci marec vydala aktualizácie opravujúce 25 zraniteľností, z toho 3 kritické. CVE-2018-5126, CVE-2018-5125 a CVE-2018-5145 sú všetko zraniteľnosťami poškodenia pamäte, ktoré môžu byť zneužité na spustenie ľubovoľného kódu.
Okrem toho boli zaznamenané ešte zraniteľnosti CVE-2018-5146 a CVE-2018-5147 cez súťaž pwn2own. Útočník vie spôsobiť písanie mimo svojej pamäte vďaka špeciálne vytvorenému súboru typu Vorbis a tak vykonať ľubovoľný škodlivý kód.

Zraniteľné systémy:

Firefox verzie 59.0.1 a staršie
Firefox ESR verzie 52.7.2 a staršie

Odporúčania:

Odporúčame aktualizovať prehliadač Mozilla Firefox na verziu 59.0.2, resp. ESR 52.7.3 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.csirt.gov.sk/oznamenia-a-varovania-803.html?id=158
https://www.mozilla.org/en-US/security/advisories/mfsa2018-06/

https://www.mozilla.org/en-US/security/advisories/mfsa2018-07/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-08/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-10/

Google Chrome

Spoločnosť Google vydala aktualizácie prehliadača Chrome, ktoré obsahujú opravy 45 bezpečnostných zraniteľností. Z toho je 9 kritických zraniteľností.

Odporúčania:

Odporúčame overiť, či sa prehliadač Chrome automaticky aktualizoval na verziu 65.0.3325.146, 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/2018/03/stable-channel-update-for-desktop.html

4. Adobe Flash Player

Tento mesiac boli vydané aktualizácie na zraniteľnosti CVE-2018-4919 a CVE-2018-4920 v Adobe Flash Playeri verzie 28.0.0.161 a starších. Obidve zraniteľnosti môžu spôsobiť spustenie kódu pod práve prihláseným používateľom. Taktiež bola vydaná aktualizácia na kritickú zraniteľnosť CVE-2018-4924 pre Adobe Dreamweaver CC, ktorá taktiež umožňuje spustenie kódu ako práve prihlásený používateľ. V marcovej aktualizácii Adobe Connect boli vyriešené dve zraniteľnosti CVE-2018-4921 a CVE-2018-4923. Jedna je chybou pri nahrávaní SWI súborov a môže byť zneužitá na cross-site scripting útoky. Druhá je spôsobená ovládačom URI v Adobe Connecte a môže mať za následok odstránenie lokálneho súboru alebo dokonca odinštalovanie aplikácie.

Zraniteľné systémy:

Adobe Flash Player Desktop Runtime 28.0.0.161 a staršie
Adobe Flash Player pre Google Chrome 28.0.0.161 a staršie
Adobe Flash Player pre Microsoft Edge a Internet Explorer 28.0.0.161 a staršie
Adobe Dreamweaver CC verzie 18.0 a staršie
Adobe Connect verzie 9.7 a staršie

Odporúčania:

Používateľom odporúčame čo najskôr aktualizovať zraniteľné systémy. Jedná sa najmä o Adobe Flash Player, ktorý treba aktualizovať na verziu 29.0.0.113, Adobe Dreamweaver CC, ktorý treba aktualizovať na verziu 18.1 a Adobe Connect, ktorý treba aktualizovať na verziu 9.7.5.
Aktualizácie sú dostupné prostredníctvom stránky Adobe Flash Player Download Center, prípadne prostredníctvom kontroly dostupných aktualizácii v produkte Adobe Flash Player.
Aktualizáciu Adobe Dreamweaveru je možné vykonať pomocou aplikácie Creative Cloud v Help menu.

Zdroje:

https://helpx.adobe.com/security/products/flash-player/apsb18-05.html
https://helpx.adobe.com/security/products/connect/apsb18-06.html
https://helpx.adobe.com/security/products/dreamweaver/apsb18-07.html
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180006

5. Frameworky

Microsoft .NET Framework

Pre tri závažné zraniteľnosti v .NET Core a ASP.NET Core boli v marci vydané aktualizácie. Zraniteľnosť CVE-2018-0875 existuje kvôli spôsobu, akým .NET Core spracováva špeciálne vytvorené požiadavky a tak spôsobuje kolíziu hashov. Útočník môže spôsobiť narušenie dostupnosti služby tak, že pošle aplikácii .NET Core malé množstvo špeciálne vytvorených požiadaviek a tak sa značne degraduje výkon.
Zraniteľnosť CVE-2018-0808 je zraniteľnosť narušenia dostupnosti služby a je spôsobená tým, že ASP.NET Core nesprávne spracúva webové požiadavky. Zraniteľnosť je možné zneužiť vzdialene bez autentifikácie. Útočník musí poslať špeciálne upravené požiadavky aplikácii .NET Core.
CVE-2018-0787 je zraniteľnosť zvýšenia práv. Nastáva tým, že zlyhá overovanie webových požiadaviek webovej aplikácie Kestrel. Na jej zneužitie je potrebné poslať webovej aplikácii špeciálne upravenú požiadavku obsahujúcu HTML injekčný kód. Tým útočník dosiahne, že sa používateľovi pošle e-mail na obnovu hesla. HTML kód by mohol byť spustený vtedy, keď používateľ otvorí e-mail.

Zraniteľné systémy:

.NET Core 1.0
.NET Core 1.1
.NET Core 2.0
PowerShell Core 6.0.0
ASP.NET Core 2.0

Odporúčania:

Vzhľadom na závažnosť uvedených zraniteľností 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/advisory/CVE-2018-0875

Oracle Java

Spoločnosť Oracle nevydala v mesiaci marec žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 17. apríl 2018.

Zdroje:

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

6. Iné závažné zraniteľnosti

AMD procesory

V marci bolo spoločnosťou CTS Labs zverejnených viacero zraniteľností týkajúcich sa AMD procesorov. Konkrétne sa jedná o zraniteľnosti: CVE-2018-8930, CVE-2018-8931, CVE-2018-8932, CVE-2018-8933,CVE-2018-8934, CVE-2018-8935, CVE-2018-8936, ktoré dávajú útočníkovi prístup k citlivým dátam, umožňujú inštalovať zotrvávajúci malvér do čipu, a získať plnú kontrolu nad systémom.
Zraniteľnosti sú rozdelené do 4 skupín útokov, pričom na zneužitie ktorejkoľvek je potrebný prístup do systému ako admin. Opravy zraniteľností skupín RyzenFall, Fallout a MasterKey chce spoločnosť uskutočniť pomocou BIOS aktualizácie. Na zraniteľnosti typu Chimera má byť vydaná záplata, ktorá ma byť taktiež zverejnená pomocou BIOS aktualizácie.
Pre bližšie informácie o jednotlivých skupinách zraniteľností si môžete prečítať naše varovanie uvedené na prvom odkaze v zdrojoch.

Zraniteľné systémy:

Procesory rady:
EPYC server
Ryzen Mobile
Ryzen Pro
Ryzen Workstation

Odporúčania:

Zatiaľ nie sú žiadne aktualizácie, spoločnosť AMD prisľúbila opravy v budúcnosti

Zdroje:

https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=159
https://amdflaws.com/
https://blog.trailofbits.com/2018/03/15/amd-flaws-technical-summary/
https://community.amd.com/community/amd-corporate/blog/2018/03/21/initial-amd-technical-assessment-of-cts-labs-research
https://safefirmware.com/amdflaws_whitepaper.pdf

Cisco

Koncom mesiaca boli objavené tri kritické zraniteľnosti v operačnom systéme IOS XE pre internú sieť od spoločnosti Cisco Systems. V polročnej správe spoločnosti Cisco Systems bolo predstavených 22 zraniteľností softvéru IOS a IOS XE z čoho 3 boli kritické.

Zraniteľnosť CVE-2018-0151 softvéru IOS a IOS XE by mohla umožniť vzdialenému neoverenému útočníkovi spôsobenie narušenia dostupnosti služby, alebo vykonanie ľubovoľného kódu so zvýšenými právami. Chyba je zapríčinená nesprávnym overovaním hraníc niektorých hodnôt v paketoch určených pre UDP port 18999. Zneužiť túto zraniteľnosť je možné posielaním škodlivých paketov zariadeniu s touto chybou. Pri spracovaní paketov môže dôjsť k pretečeniu zásobníka. Aktualizácie pre túto zraniteľnosť už boli vydané spoločnosťou Cisco.

Zraniteľnosť CVE-2018-0171 je chybou funkcie Smart Install softvéru Cisco IOS a IOS XE. Chyba overovania paketových dát môže byť zneužitá tým, že útočník pošle škodlivú správu funkcie Smart Install na TCP port 4786. Úspešne vykonaný útok umožní útočníkovi dosiahnuť

pretečenie zásobníka na zariadení, čo dovolí spustenie kódu na diaľku alebo spôsobenie nekonečnej slučky. Pre zabezpečenie tejto chyby odporúčame vypnúť funkciu Smart Install.

Zraniteľnosť CVE-2018-0150 softvéru Cisco IOS XE je spôsobená neregistrovaným používateľským účtom s oprávneniami úrovne 15, ktorý má predvolené meno a heslo. Útočník môže tento účet použiť na vzdialené pripojenie ku zariadeniu s príslušnou verziou softvéru Cisco IOS XE. Takto sa pri úspešnom zneužití vie útočník prihlásiť do daného zariadenia s oprávneniami úrovne 15. Cisco IOS má 16 úrovní práv, pričom úroveň 15 zodpovedá root oprávneniam. Zraniteľnými sú zariadenia s verziou softvéru Cisco IOS XE Release 16.x., ale chyba neovplyvňuje zariadenia so skoršími vydaniami softvéru. Správcovia majú možnosť sa zbaviť tejto chyby odstránením predvoleného účtu pomocou príkazu 'no username cisco'. Taktiež zmenou hesla pre tento účet vedia administrátori zabezpečiť túto chybu.

Zraniteľné systémy:

Cisco IOS XE release 16.x.
Cisco IOS Software
Cisco IOS XE Software

Odporúčania:

Boli vydané záplaty na dve z týchto zraniteľností. Na prvých troch linkoch v zdrojoch sa nachádza návod pre administrátorov, ako zistiť či sú dané zariadenia ovplyvňované spomínanými zraniteľnosťami. Taktiež sú tam popísané postupy ako zabezpečiť systémy.

Zdroje:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-qos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-xesc
https://threatpost.com/cisco-patches-two-critical-rce-bugs-in-ios-xe-software/130852/