Mesačný prehľad kritických zraniteľností
Máj 2018

1. Operačné systémy Microsoft Windows

V máji spoločnosť Microsoft opravila 4 kritické zraniteľnosti operačného systému Microsoft Windows.
Zraniteľnosti CVE-2018-0959 a CVE-2018-0961 môžu spôsobiť vykonanie škodlivého kódu na diaľku. Prvá z nich je spôsobená nesprávnym overovaním vstupu Windows Hyper-V na serveri od autentifikovaného používateľa na hostiteľskom operačnom systéme. Druhá sa týka overovania paketových dát v SMB protokole systému Windows Hyper-V. Na zneužitie týchto zraniteľností musí útočník spustiť špeciálne vytvorenú aplikáciu, ktorá umožní zneužitie týchto zraniteľností. Úspešný útočník následne môže vykonať ľubovoľný kód pomocou Windows Hyper-V.
Našli sa aj zraniteľnosti CVE-2018-8120 a CVE-2018-8174 taktiež umožňujúce vzdialené vykonávanie kódu či zvýšenie privilégií, ktoré sú bližšie popísané aj v našom varovaní.

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 10 Version 1803 for 32-bit Systems
Windows 10 Version 1803 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)
Windows Server, version 1803 (Server Core installation)

Odporúčania:

Vzhľadom na množstvo kritických 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-2018-8174
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0959
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0961
https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=170

2. Kancelárske balíky Microsoft Office a Office Web Apps

Únik zašifrovaných mailov môžu spôsobiť zraniteľnosti CVE-2017-17688 a CVE-2017-17689, ktoré sú bližšie popísané v našom varovaní.

Závažné zraniteľnosti CVE-2018-8147, CVE-2018-8148, CVE-2018-8157, CVE-2018-8158, CVE-2018-8161, CVE-2018-8162, CVE-2018-8173 a CVE-2018-8176 spôsobené nesprávnym narábaním s objektmi v pamäti umožňujú útočníkovi spúšťať kód na diaľku. Útočník na ich zneužitie môže použiť špeciálne vytvorenú stránku, no musí presvedčiť používateľa, aby ju navštívil. To môže urobiť zaslaním mailu alebo okamžitej správy s odkazom, na ktorý má používateľ kliknúť. Prípadne by mohol útočník využiť aj špeciálne vytvorený súbor navrhnutý na zneužitie zraniteľnosti. Aj v tomto prípade však musí útočník presvedčiť používateľa aby otvoril súbor. Pri úspešnom zneužití niektorej z týchto zraniteľností, môže útočník získať právo spúšťať škodlivý kód ako práve prihlásený používateľ. V prípade, že bol používateľ prihlásený ako administrátor získa útočník možnosť inštalovať programy, zobrazovať, meniť alebo mazať dáta, či vytvárať plnohodnotné účty.

Ďalšími závažnými zraniteľnosťami sú CVE-2018-8149, CVE-2018-8155, CVE-2018-8156, CVE-2018-8168, ktoré môžu spôsobiť zvýšenie práv tým, že Microsoft SharePoint Server nesprávne spracuje špeciálne vytvorenú webovú požiadavku na SharePoint Server. Útočník túto zraniteľnosť môže zneužiť poslaním špeciálne upravenej URL adresy používateľovi zasiahnutého SharePoint servera. Po úspešnom zneužití niektorej z týchto zraniteľností môže útočník vykonať cross-site scripting útoky na zraniteľných systémoch a spúšťať skripty ako práve prihlásený používateľ. To umožní útočníkovi čítať obsah, na ktorý nemá právo,

vykonávať akcie v službe SharePoint ako daný používateľ (napríklad zmena alebo odstránenie obsahu či vložiť škodlivý obsah do prehliadača používateľa).
Zraniteľnosť CVE-2018-8160 je závažná a môže spôsobiť únik citlivých informácií. Na jej zneužitie je potrebné otvoriť škodlivý email poslaný útočníkom. Tým sa automaticky vytvorí pripojenie k vzdialenému serveru SMB protokolom. Útočník teraz môže urobiť útok hrubou silou na odpoveď protokolu NTLM a odhaliť zodpovedajúci hash hesla.
Únik citlivých informácii môže nastať aj v Microsoft Exceli (CVE-2018-8163) pri nesprávnom zverejňovaní pamäte. Ako pri väčšine týchto zraniteľností, na jej zneužitie potrebuje útočník interakciu používateľa. Potrebuje ho totiž presvedčiť aby otvoril špeciálne vytvorený dokument, ktorý mu môže poslať napríklad e-mailom. Útočník v tomto prípade taktiež potrebuje poznať lokáciu, kde bol objekt vytvorený v pamäti.

Zraniteľné systémy:

Microsoft Sharepoint enerprise Server 2016
Microsoft Project Server 2010 Service Pack 2
Microsoft Project Server 2013 Service Pack 1
Microsoft SharePoint Foundation 2013 Service Pack 1
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 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 2 (32-bit editions)
Microsoft Office 2013 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
Outlook 2007 (12.0.4518.1014)
Outlook 2010 (14.0.7190.5000)
Outlook 2013 (15.0.4989.1000)
Outlook 2016 (16.0.4266.1001)

Win. 10 Mail (17.8730.21865.0)
Win. Live Mail (16.4.3528.0331)

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-2018-8162
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8148
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8147
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8163
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8149
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8155
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8156
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8157
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8158
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8160
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8161
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8168
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8176
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8173

3. Internetové prehliadače

Microsoft Internet Explorer

V rámci májového balíka opráv boli spoločnosťou Microsoft vydané opravy 6 kritických zraniteľností.
To, ako skriptovací engine narába s objektmi v pamäti, môže spôsobiť zraniteľnosť vzdialeného vykonávania kódu. Konkrétne sa jedná o zraniteľnosti označené CVE-2018-8114, CVE-2018-8122, CVE-2018-1022, CVE-2018-0955, CVE-2018-8178 a CVE-2018-0954. Útočník, ktorý úspešne zneužije jednu z týchto zraniteľností môže poškodiť pamäť takým spôsobom, že získa možnosť vzdialene vykonávať ľubovoľný kód s právami ako práve prihlásený používateľ. Používateľ využívajúci administrátorské práva tak umožní úspešnému útočníkovi inštalovať programy, prezerať, mazať alebo meniť dáta, či vytvárať ďalšie plnohodnotné účty. Útočník potrebuje presvedčiť používateľa aby navštívil špeciálne vytvorenú stránku, ktorej odkaz môže útočník poslať napríklad pomocou emailu alebo rýchlej správy. Taktiež má možnosť vložiť do aplikácie alebo dokumentu Microsoft Office prvok ActiveX označený ako bezpečný na inicializáciu.

Zraniteľné systémy:

Microsoft Internet Explorer verzie 10 a 11

Odporúčania:

Vzhľadom množstvo kritických 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-2018-1022
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0954
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0955
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8114
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8122
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8178

Microsoft Edge

V máji bola zverejnená aktualizácia, ktorá opravuje viacero kritických zraniteľností pričom všetky umožňujú vykonať škodlivý kód na diaľku.
Sú spôsobené tým, že skriptovací engine nesprávne narába s objektmi v pamäti. Zneužitie je možné len za pomoci používateľa, ktorého musí útočník presvedčiť k navštíveniu ním špeciálne vytvorenej stránky. 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.

Zraniteľné systémy:

Microsoft Edge v systémoch Windows 10 verzií 1607, 1703, 1709 a 1803 a 32-bitových aj 64-bitových verziách
Microsoft Edge v systéme Windows Server 2016

Odporúčania:

Vzhľadom na množstvo kritických 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-2018-0943
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8133
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8130
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0945
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0946
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0951

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8137
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8193
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8128
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0953

Mozilla Firefox

Spoločnosť Mozilla v máji vydala aktualizácie opravujúce mnoho zraniteľností, z čoho 3 kritické. CVE-2018-5150, CVE-2018-5151 sú zraniteľnosťami poškodenia pamäte, ktoré môžu byť zneužité na spustenie ľubovoľného kódu. Mozilla taktiež opravila problém poškodenia pamäte a neplatného čítania vyrovnávacej pamäte pri grafických operáciách umožňujúci zraniteľnosť CVE-2018-5183 spôsobený knižnicou Skia.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-13/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-12/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-11/

Google Chrome

Spoločnosť Google vydala aktualizácie prehliadača Chrome, ktoré obsahujú opravy 4 bezpečnostných zraniteľností. Z toho je 1 kritická a 3 sú závažné zraniteľnosti.

Odporúčania:

Odporúčame overiť, či sa prehliadač Chrome automaticky aktualizoval na verziu 66.0.3359.170, 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/2018/05/stable-channel-update-for-desktop.html

4. Adobe Flash Player

Tohto mesiaca boli vydané aktualizácie na tri kritické zraniteľnosti CVE-2018-4944 v Adobe Flash Playeri verzie 29.0.0.140 a starších. Tieto zraniteľnosti môžu spôsobiť spustenie kódu ako práve prihlásený používateľ. V Acrobat Readeri bolo tento mesiac opravených až 23 kritických zraniteľností pričom sú zverejnené exploity na niektoré z nich. Každá z týchto zraniteľností umožňuje vzdialené vykonávanie ľubovoľného kódu.

Zraniteľné systémy:

Adobe Flash Player Desktop Runtime 29.0.0.140 a staršie
Adobe Flash Player pre Google Chrome 29.0.0.140 a staršie
Adobe Flash Player pre Microsoft Edge a Internet Explorer 29.0.0.140 a staršie
Acrobat DC Continuous verzie 2018.011.20038 a staršie
Acrobat Reader DC verzie 2018.011.20038 a staršie

Acrobat 2017 verzie 2017.011.30079 a staršie
Acrobat Reader DC 2017 verzie 2017.011.30079 a staršie
Acrobat DC (Classic 2015) verzie 2015.006.30417 a staršie
Acrobat Reader DC (Classic 2015) verzie 2015.006.30417 a staršie

Odporúčania:

Používateľom odporúčame čo najskôr aktualizovať zraniteľné systémy. Jedná sa najmä. o Adobe Flash Player, ktorý treba aktualizovať na verziu 29.0.0.171. Aktualizácie sú dostupné prostredníctvom stránky Adobe Flash Player Download Center, prípadne prostredníctvom kontroly dostupných aktualizácii v produkte Adobe Flash Player.
Vzhľadom na množstvo kritických zraniteľností a fakt, že na niektoré sú zverejnené exploity, odporúčame urýchlene aktualizovať aj Acrobat reader nasledovne:

- Acrobat DC na verziu 2018.011.20040
- Acrobat Reader DC na verziu 2018.011.20040
- Acrobat 2017 na verziu 2017.011.30080
- Acrobat Reader DC 2017 na verziu 2017.011.30080
- Acrobat Reader DC (Classic 2015) na verziu 2015.006.30418
- Acrobat DC (Classic 2015) na verziu 2015.006.30418

Pričom na prvom linku z zdrojoch môžete nájsť odkazy na stiahnutie pre jednotlivé systémy.

Zdroje:

https://helpx.adobe.com/security/products/acrobat/apsb18-09.html
https://helpx.adobe.com/security/products/flash-player/apsb18-16.html

5. Frameworky

Microsoft .NET Framework

Pre Microsoft .NET Framework boli vydané aktualizácie opravujúce dve závažné zraniteľnosti. Narušenie dostupnosti systému môže byť spôsobená zraniteľnosťou CVE-2018-0765, ktorá nastáva pri nesprávnom spracovaní XML dokumentov. Na jej zneužitie môže útočník použiť špeciálne vytvorené požiadavky pre .NET aplikáciu. Druhou zraniteľnosťou je CVE-2018-1039 po ktorej zneužití má útočník možnosť obísť politiku UCMI (User Mode Code Integrity) na zariadení. Na jej zneužitie potrebuje útočník spustiť škodlivý kód na lokálnom počítači, čo znamená, že k nemu najprv potrebuje prístup.

Zraniteľné systémy:

Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.0 Service Pack 2
Microsoft .NET Framework 3.5 Service Pack 2
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 4.5.2
Microsoft .NET Framework 4.6
Microsoft .NET Framework 4.6.1
Microsoft .NET Framework 4.6.2
Microsoft .NET Framework 4.7
Microsoft .NET Framework 4.7.1
Microsoft .NET Framework 4.7.2

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0765
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1039

Oracle Java

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

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

6. Iné závažné zraniteľnosti

EFAIL

Zraniteľnosť pri šifrovaní e-mailov PGP a S/MIME umožňuje únik šifrovaných e-mailov a následné rozšifrovania. Zraniteľnosť je bližšie popísaná v našom varovaní.

Zraniteľné systémy:

Windows
Outlook 2007 (12.0.4518.1014)
Outlook 2010 (14.0.7190.5000)
Outlook 2013 (15.0.4989.1000)
Outlook 2016 (16.0.4266.1001)
Win. 10 Mail (17.8730.21865.0)
Win. Live Mail (16.4.3528.0331)
The Bat! (8.2.0)
Postbox (5.0.20)
eM Client (7.1.31849.0)
IBM Notes (9.0.1)
Pegasus Mail (4.72.572)

Linux
Thunderbird (52.5.2)
Evolution (3.22.6)
Trojitá(0.7-278)
KMail (5.2.3)
Claws (3.14.1)
Mutt (1.7.2)

macOS
Apple Mail (11.2)
MailMate (1.10)
Airmail (3.5.3)

iOS
Mail App (11.2.2)
Canary Mail (1.17)

Android
K-9 Mail (5.403)
R2Mail2 (2.30)
MailDroid (4.81)
Nine (4.1.3a)

Webmail
Mailbox.org
Hushmail
ProtonMail
Mailfence
GMail
Outlook.com
iCloud Mail
Webapp
Roundcube (1.3.4)
AfterLogic (7.7.9)
Rainloop (1.11.3)
Mailpile (1.0.0rc2)

Groupware
Exchange OWA (15.1.1034.32)
GroupWise (14.2.2)
Horde (5.2.22/IMP 6.2.21)

Odporúčania:
Návody na záplaty pre niektorých e-mailových klientov sú taktiež vypísané v našom varovaní.

Zraniteľnosť v knižnici hcsshim

Zraniteľnosť objavená v knižnici Windows Host Compute Service Shim umožňuje po zneužití vzdialené vykonávanie kódu. Pre bližšie informácie si pozrite naše varovanie.

Zraniteľné systémy:
Hcsshim verzie staršej ako 0.6.10

Odporúčania:
Vo verzii 0.6.10 je zraniteľnosť opravená. Odporúčame teda aktualizovať na túto verziu.

Cisco DNA Center

V Cisco Digital Network Architecture Center boli objavené zraniteľnosti umožňujúce zvýšenie privilégií či spúšťanie príkazov s root oprávneniami. Viac informácií môžete získať v našom varovaní.

Zraniteľné systémy:
Cisco DNA Center Software verzie 1.1.3. alebo staršej

Odporúčania:
Aktualizácie opravujúce tieto zraniteľnosti už boli vydané a môžete ich nájsť v Cisco cloude, prípadne pre administrátorov je tu možnosť využiť System Update softvéru. Odporúčame aktualizovať Cisco DNA Center na verziu 1.1.4. alebo neskoršiu.

Citrix WebEx

Vzdialené vykonávanie kódu v Cisco WebEx Recording Player for Advanced Recording Format (ARF) je možné kvôli nájdeným zraniteľnostiam o ktorých sa môžete viac dočítať v našom varovaní.

Zraniteľné systémy:
Cisco WebEx Network Recording Player 0
Cisco WebEx Meetings Server 3.0
Cisco WebEx Meetings Server 2.8
Cisco WebEx Meetings Server 2.7
Cisco Webex Meetings Online T31.20
Cisco Webex Meetings Online T31
Cisco WebEx Meetings Client T31.14
Cisco WebEx Business Suite (WBS32) client T32.2
Cisco WebEx Business Suite (WBS32) client T32.10
Cisco WebEx Business Suite (WBS31) client T31.23.2
Cisco WebEx Business Suite (WBS31) client T31.14.1
Cisco WebEx Business Suite (WBS31) client T31.10

Odporúčania:
Pre Cisco WebEx Business Suite meeting sites, Cisco WebEx Meetings sites, Cisco WebEx Meetings Server a Cisco WebEx ARF Player boli vydané aktualizácie, ktoré odporúčame inštalovať. Odkazy na návody a aktualizácie môžete nájsť v odporúčaniach nášho varovania.