BEZPEČNOSTNÝ BULLETIN

Týždeň 18. 07. 2018 – 24. 07. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	RSA Archer Multiple Vulnerabilities	Vysoká	**8.8**
02.	Foxit PDF Reader and PhantomPDF Multiple Vulnerabilities	Vysoká	**8.8**
03.	Cisco Products Multiple Vulnerabilities	Vysoká	**8.8**
04.	ACD Systems Canvas Draw 4 Multiple Vulnerabilities	Vysoká	**8.8**
05.	Moxa NPort 5210, 5230 and 5232 Denial of Service Vulnerability	Vysoká	**7.5**
06.	XMLSoft libxml2 Denial of Service Vulnerability	Vysoká	**7.5**
07.	F5 BIG-IP Multiple Vulnerabilities	Vysoká	**7.5**
08.	Bluetooth Validation Vulnerability	Vysoká	**7.4**
09.	Apache Releases Security Updates for Apache Tomcat	Stredná	**5.3**
10.	Apache HTTP Server Multiple Vulnerabilities	Stredná	**5.3**

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2915*

SK-CERT
Naša značka:
02049/2018/TS/OKB-098

BEZPEČNOSTNÝ BULLETIN

Týždeň 18. 07. 2018 – 24. 07. 2018

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

RSA Archer Multiple Vulnerabilities

Popis

Spoločnosť RSA vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produkte RSA Archer.
Najzávažnejšia zraniteľnosť spočíva v implementačnej chybe v REST API a vzdialený autentifikovaný útočník by ju mohol zneužiť na eskaláciu privilégií.
Druhá zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený autentifikovaný útočník by ju mohol zneužiť na realizáciu XSS (Cross-Dite Scripting) útoku, vykonanie škodlivého kódu vo webovom prehliadači a získanie prístupu k údajom uloženým v cookies, vrátane autentifikačných údajov.

Dátum prvého zverejnenia varovania

18.07.2018

CVE

CVE-2018-11059, CVE-2018-11060

Zasiahnuté systémy

RSA Archer verzie staršie ako 6.1.0.3
RSA Archer verzie staršie ako 6.2.0.10
RSA Archer verzie staršie ako 6.3.0.7
RSA Archer verzie staršie ako 6.4.0.1

Následky

Vykonanie škodlivého kódu, Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://seclists.org/fulldisclosure/2018/Jul/69
https://exchange.xforce.ibmcloud.com/vulnerabilities/147141
https://exchange.xforce.ibmcloud.com/vulnerabilities/147142

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Foxit PDF Reader and PhantomPDF Multiple Vulnerabilities

Popis

Spoločnosť Foxit vydala bezpečnostné aktualizácie na svoje produkty Foxit PDF Reader a Foxit PhantomPDF, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti spočívajú v implementačných chybách vo viacerých metódach, nesprávnom spracovaní anotácií a parsovaní súborov.
Uvedené zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vykonanie škodlivého kódu v kontexte bežiaceho procesu.

Dátum prvého zverejnenia varovania

19.07.2018

CVE

CVE-2018-11617, CVE-2018-11618, CVE-2018-11619, CVE-2018-11620, CVE-2018-11621, CVE-2018-11622, CVE-2018-11623, CVE-2018-14241, CVE-2018-14242, CVE-2018-14243, CVE-2018-14244, CVE-2018-14245, CVE-2018-14246, CVE-2018-14247, CVE-2018-14248, CVE-2018-14249, CVE-2018-14250, CVE-2018-14251, CVE-2018-14252, CVE-2018-14253, CVE-2018-14254, CVE-2018-14255, CVE-2018-14256, CVE-2018-14257, CVE-2018-14258, CVE-2018-14259, CVE-2018-14260, CVE-2018-14261, CVE-2018-14262, CVE-2018-14263, CVE-2018-14264, CVE-2018-14265, CVE-2018-14266, CVE-2018-14267, CVE-2018-14268, CVE-2018-14269, CVE-2018-14270, CVE-2018-14271, CVE-2018-14272, CVE-2018-14273, CVE-2018-14274, CVE-2018-14275, CVE-2018-14276, CVE-2018-14277, CVE-2018-14277, CVE-2018-14278, CVE-2018-14278, CVE-2018-14279, CVE-2018-14279, CVE-2018-14280, CVE-2018-14280, CVE-2018-14281, CVE-2018-14281, CVE-2018-14282, CVE-2018-14282, CVE-2018-14283, CVE-2018-14283, CVE-2018-14284, CVE-2018-14284, CVE-2018-14285, CVE-2018-14286, CVE-2018-14287, CVE-2018-14288, CVE-2018-14289, CVE-2018-14290, CVE-2018-14290, CVE-2018-14291, CVE-2018-14292, CVE-2018-14292, CVE-2018-14293, CVE-2018-14293, CVE-2018-14294, CVE-2018-14294, CVE-2018-14295, CVE-2018-14295, CVE-2018-14296, CVE-2018-14297, CVE-2018-14298, CVE-2018-14299, CVE-2018-14300, CVE-2018-14301, CVE-2018-14301, CVE-2018-14302, CVE-2018-14302, CVE-2018-14303, CVE-2018-14303, CVE-2018-14304, CVE-2018-14304, CVE-2018-14305, CVE-2018-14305, CVE-2018-14306, CVE-2018-14306, CVE-2018-14307, CVE-2018-14307, CVE-2018-14308, CVE-2018-14308, CVE-2018-14309, CVE-2018-14310, CVE-2018-14311, CVE-2018-14312, CVE-2018-14313, CVE-2018-14314, CVE-2018-14315, CVE-2018-14316, CVE-2018-14258, CVE-2018-3924, CVE-2018-3939

Zasiahnuté systémy

Foxit Reader verzie staršie ako 9.2

Foxit PhantomPDF verzie staršie ako 9.2

Následky
Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://www.foxitsoftware.com/support/security-bulletins.php https://blog.talosintelligence.com/2018/07/vuln-spotlight-foxit-rce.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Cisco Products Multiple Vulnerabilities

Popis

Spoločnosť Cisco vydala súbor bezpečnostných aktualizácií, ktoré opravujú viacero zraniteľností v ich produktovom portfóliu.

Najzávažnejšie bezpečnostné zraniteľnosti v produkte Cisco SD-WAN Solution spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému autentifikovanému útočníkovi vykonať škodlivý kód na napadnutom systéme.

Bezpečnostné zraniteľnosti v produkte Cisco Webex Network Recording Player umožňujú vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených ARF a WRF vykonať škodlivý kód na zasiahnutom systéme.

Najvážnejšia zraniteľnosť v prepínačoch Cisco Nexus 9000 umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených DHCPv6 paketov spôsobiť odopretie služieb.

Dátum prvého zverejnenia varovania

18.07.2018

CVE

CVE-2018-0342, CVE-2018-0343, CVE-2018-0344, CVE-2018-0345, CVE-2018-0346, CVE-2018-0347, CVE-2018-0348, CVE-2018-0349, CVE-2018-0350, CVE-2018-0351, CVE-2018-0372, CVE-2018-0379, CVE-2018-0380, CVE-2018-0387, CVE-2018-0390, CVE-2018-0394, CVE-2018-0396, CVE-2018-0398, CVE-2018-0399, CVE-2018-0400, CVE-2018-0401, CVE-2018-0402, CVE-2018-0403

Zasiahnuté systémy

Cisco SD-WAN Solution running on vBond Orchestrator Software
Cisco SD-WAN Solution running on vEdge 100 Series Routers
Cisco SD-WAN Solution running on vEdge 1000 Series Routers
Cisco SD-WAN Solution running on vEdge 2000 Series Routers
Cisco SD-WAN Solution running on vEdge 5000 Series Routers
Cisco SD-WAN Solution running on vEdge Cloud Router Platform
Cisco SD-WAN Solution running on vManage Network Management Software
Cisco SD-WAN Solution running on vSmart Controller Software
Cisco Finesse
Cisco Cloud Service Platform 2100
Cisco Unified Communications Manager IM & Presence Service
Cisco Unified Contact Center Express (Unified CCX)
Cisco WebEx
Cisco Webex Teams for MacOS

Cisco Webex Meetings Suite (WBS31) - Webex Network Recording Player and Webex Player versions prior to WBS31.23
Cisco Webex Meetings Suite (WBS32) - Webex Network Recording Player and Webex Player versions prior to WBS32.15
Cisco Webex Meetings Suite (WBS33) - Webex Network Recording Player and Webex Player versions prior to WBS33.2
Cisco Webex Meetings Online - Webex Network Recording Player and WebEx Player versions prior to 1.3.35
Cisco Webex Meetings Server - Webex Network Recording Player versions prior to 3.0MR1
Cisco Nexus 9000 Series Fabric Switches

Následky
Vykonanie škodlivého kódu, Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom, Neoprávnená zmena v systéme, Eskalácia privilégií

Odporúčania
Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-cisco-products-could-allow-for-remote-code-execution_2018-082/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

ACD Systems Canvas Draw 4 Multiple Vulnerabilities

Popis

Spoločnosť Canvas GFX vydala bezpečnostnú aktualizáciu na svoj produkt Canvas Draw 4, ktoré opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti spočívajú v nesprávnom parsovaní súborov a vzdialený neautentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne vytvorených .tiff a .pcx súborov mohol zneužiť na vykonanie škodlivého kódu v kontexte bežiaceho procesu.

Dátum prvého zverejnenia varovania

19.07.2018

CVE

CVE-2018-3857, CVE-2018-3858, CVE-2018-3859, CVE-2018-3860, CVE-2018-3870, CVE-2018-3871,

Zasiahnuté systémy

ACDSystems Canvas Draw 4.0.0

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov

Zdroje

https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0553
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0544
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0552
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0541
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0542
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0543

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.5**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Moxa NPort 5210, 5230 and 5232 Denial of Service Vulnerability

Popis

Spoločnosť Moxa vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť v sériových sieťových rozhraniach NPort 5210, 5230 a 5232.
Bližšie nešpecifikované zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom zasielania veľkého množstva TCP SYN paketov mohol zneužiť na zahltenie prostriedkov zariadenia a následné zneprístupnenie služby.

Dátum prvého zverejnenia varovania

19.07.2018

CVE

CVE-2018-10632

Zasiahnuté systémy

Moxa NPort 5210, 5230, 5232 Verzie 2.9 build 17030709 a staršie

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu firmvéru zasiahnutých zariadení, aplikovať firewallové pravidlá a limitovať prístup k zariadeniam a ich funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-200-04
https://exchange.xforce.ibmcloud.com/vulnerabilities/147138

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.5**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

XMLSoft libxml2 Denial of Service Vulnerability

Popis

Knižnica XMLSoft libxml2 na parsovanie XML dokumentov obsahuje bezpečnostnú zraniteľnosť. Zraniteľnosť spočívajúcu v nesprávnom parsovaní neplatných XPath výrazov vo funkcii xmlXPathCompOpEval() by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvoreného XML súboru mohol zneužiť na zneprístupnenie služieb aplikácií využívajúcich knižnicu libxml2. Na uvedenú zraniteľnosť je voľne dostupný exploit.

Dátum prvého zverejnenia varovania

19.07.2018

CVE

CVE-2018-14404

Zasiahnuté systémy

libxml2 verzie 2.5, 2.6, 2.7, 2.8 a 2.9

Následky

Zneprístupnenie služby

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=58450
https://gitlab.gnome.org/GNOME/libxml2/issues/10

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.5**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

F5 BIG-IP Multiple Vulnerabilities

Popis

Spoločnosť F5 vydala bezpečnostné aktualizácie na svoj produkt BIG-IP, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti spočívajú v nesprávnom spracovaní SSL paketov v komponente TMM (Traffic Management Microkernel) a vzdialený neautentifikovaný útočník by ich mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

18.07.2018

CVE

CVE-2018-5532, CVE-2018-5533, CVE-2018-5534, CVE-2018-5535

Zasiahnuté systémy

F5 BIG-IP

Následky

Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.f5.com/csp/article/K48224824
https://support.f5.com/csp/article/K19634255
https://support.f5.com/csp/article/K64552448
https://support.f5.com/csp/article/K45325728

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.5**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bluetooth Validation Vulnerability

Popis

Výskumníci z Izraelského technologického inštitútu vydali upozornenie na bezpečnostnú zraniteľnosť, ktorá sa nachádza v implementáciách bluetooth technológie v zariadeniach viacerých výrobcov.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním parametrov eliptických kriviek využívaných na generovanie verejných kľúčov pri nadväzovaní spojenia. Zraniteľnosť umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia neplatného verejného šifrovacieho kľúča zrealizovať MITM (man-in-the-middle) útok a získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

23.07.2018

CVE

CVE-2018-5383

Zasiahnuté systémy

Implementácie Bluetooth technológie v zariadeniach Apple, Broadcom, Intel, QUALCOMM Incorporated a iných

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Výrobcovia zasiahnutých systémov v súčasnej dobe vydávajú aktualizácie pre svoje produkty. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://www.kb.cert.org/vuls/id/304725
https://exchange.xforce.ibmcloud.com/vulnerabilities/147216

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache Releases Security Updates for Apache Tomcat

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt Apache Tomcat, ktorá opravuje dvojicu bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť spočíva v nesprávnom ukončovaní nadviazaného spojenia a vzdialený neautentifikovaný útočník by ju mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom.
Druhá zraniteľnosť spočíva v nesprávnom spracovaní niektorých UTF-8 znakov a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

22.07.2018

CVE

CVE-2018-1336, CVE-2018-8037

Zasiahnuté systémy

Apache Tomcat verzie staršie ako 9.0.10
Apache Tomcat verzie staršie ako 8.5.32

Následky

Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C20180722090623.GA92700%40minotaur.apache.org%3E
http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C20180722090435.GA60759%40minotaur.apache.org%3E
https://exchange.xforce.ibmcloud.com/vulnerabilities/147212

BEZPEČNOSTNÝ BULLETIN

Týždeň 18. 07. 2018 – 24. 07. 2018

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache HTTP Server Multiple Vulnerabilities

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt Apache HTTP Server, ktorá opravuje dvojicu bezpečnostných zraniteľností spočívajúcich v nesprávnom spracovaní HTTP a HTTP/2 požiadaviek.

Najzávažnejšia zraniteľnosť sa nachádza v komponente mod_md a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených HTTP požiadaviek mohol zneužiť na vyvolanie SEGFAULT chyby a následné zneprístupnenie služby.

Druhá zraniteľnosť spočíva v nesprávnej alokácii workerov a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených HTTP/2 požiadaviek mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

18.07.2018 (posledná aktualizácia 19.07.2018)

CVE

CVE-2018-1333, CVE-2018-8011

Zasiahnuté systémy

Apache HTTP Server verzie 2.4.20, 2.4.23, 2.4.25, 2.4.26, 2.4.27, 2.4.28, 2.4.29, 2.4.30, 2.4.33

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2018-1333
https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2018-8011
https://tools.cisco.com/security/center/viewAlert.x?alertId=58444
https://tools.cisco.com/security/center/viewAlert.x?alertId=58443

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2915*

SK-CERT
Naša značka:
02049/2018/TS/OKB-098