BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 02. 2018 – 13. 02. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Číslo	Identifikátor	Dôležitosť	CVSS Skóre
1	Cisco RV132W and RV134W Multiple Vulnerabilities	Kritická	9.8
2	Cisco Products Multiple Vulnerabilites	Vysoká	8.8
3	IBM WebSphere Potential Privilege Escalation	Vysoká	8.8
4	Exim base64d Function Buffer Overflow Arbitrary Code Execution Vulnerability	Vysoká	8.1
5	FFmpeg Denial of Service Vulnerability	Vysoká	7.5
6	F5 BIG-IP Policy Enforcement Manager URL Categorization Denial of Service Vulnerability	Vysoká	7.5
7	PostgreSQL Denial of Service and Information Disclosure vulnerabilities	Vysoká	7.1
8	Brocade Fabric OS Multiple Vulnerabilities	Stredná	6.5
9	Cisco Data Center Analytics Cross-Site Scripting Vulnerabilities	Stredná	6.1

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2858*

SK-CERT
Naša značka:
02049/2018/TS/OKB-004

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☐ **Vysoká**	☒ **Kritická**	**CVSS skóre: 9.8**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Cisco RV132W and RV134W Multiple Vulnerabilities

Popis

Webové rozhranie smerovačov RV132W ADSL2+ Wireless-N VPN Router a RV134W VDSL2 Wireless-AC VPN Router od spoločnosti Cisco obsahuje viacero zraniteľností.
Najkritickejšia spočíva v nesprávnom overovaní používateľských vstupov HTTP požiadaviek a vzdialený neautentifikovaný útočník by ju mohol zneužiť na vykonanie škodlivého kódu a následné získanie úplnej kontroly nad systémom.
Ďalšia zraniteľnosť spočíva v chýbajúcich mechanizmoch autentifikácie používateľov niektorých stránok webového rozhrania smerovačov. Vzdialený neautentifikovaný útočník by ju mohol zneužiť na prístup ku konfigurácii zariadenia, vrátane hesla pre administrátorský prístup.

Dátum prvého zverejnenia varovania

07.02.2018

CVE

CVE-2018-0125, CVE-2018-0127

Zasiahnuté systémy

RV132W ADSL2+ Wireless-N VPN Router
RV134W VDSL2 Wireless-AC VPN Router

Následky

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

Odporúčania

Spoločnosť Cisco vydala aktualizácie, ktoré riešia predmetnú zraniteľnosť. Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://www.us-cert.gov/ncas/current-activity/2018/02/07/Cisco-Releases-Security-Updates-Multiple-Products
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180207-rv13x
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180207-rv13x_2

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

Identifikátor

Cisco Products Multiple Vulnerabilites

Popis

Viacero produktov od spoločnosti Cisco obsahuje bezpečnostné zraniteľnosti, ktoré by vzdialený útočník mohol zneužiť na obídenie mechanizmov autentifikácie, získanie neoprávneného prístupu k citlivým údajom alebo zneprístupnenie služby.
Zraniteľnosti sú spôsobené nesprávnym overovaním používateľských vstupov a nedostatočnou implementáciou zabezpečenia údajov uložených v databáze.

Dátum prvého zverejnenia varovania

07.02.2018

CVE

CVE-2018-0113, CVE-2018-0116, CVE-2018-0117, CVE-2018-0119, CVE-2018-0120, CVE-2018-0123, CVE-2018-0132, CVE-2018-0134, CVE-2018-0135, CVE-2018-0137, CVE-2018-0140, CVE-2018-0198

Zasiahnuté systémy

Cisco UCS Central Software, Cisco Virtualized Packet Core−Distributed Instance (VPC−DI) Software, Cisco Policy Suite, Cisco Unified Communications Manager, Cisco Spark, Cisco IOS XR Software, Cisco Firepower System Software, Cisco Email Security Appliance and Cisco Content Security Management Appliance, Cisco Prime Network

Následky

Narušenie dôvernosti, integrity a dostupnosti zasiahnutých systémov

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.us-cert.gov/ncas/current-activity/2018/02/07/Cisco-Releases-Security-Updates-Multiple-Products
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180207-ucsc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180207-cps
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180207-vpcdi

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

Identifikátor

IBM WebSphere Potential Privilege Escalation

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt WebSphere Application Server, ktorá opravuje bezpečnostné zraniteľnosti v administrátorskej konzole.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných opatrení a umožňuje vzdialenému autentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

29.01.2018

CVE

CVE-2017-1681, CVE-2017-1731

Zasiahnuté systémy

IBM WebSphere Application Server 7.0, 8.0, 8.5, 9.0

Následky

Eskalácia privilégií, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://www-01.ibm.com/support/docview.wss?uid=swg22012345
https://tools.cisco.com/security/center/viewAlert.x?alertId=56769
https://tools.cisco.com/security/center/viewAlert.x?alertId=56768

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Exim base64d Function Buffer Overflow Arbitrary Code Execution Vulnerability

Popis

Vývojári e-mailového agenta Exim vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v *base64d* funkcii v SMTP komponente.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov zasiahnutým systémom a umožňuje vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne upravenej správy spôsobiť pretečenie zásobníka a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

09.02.2018

CVE

CVE-2018-6789

Zasiahnuté systémy

Exim verzie 4.80, 4.82 až 4.90

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých.

Zdroje

https://exim.org/static/doc/security/CVE-2018-6789.txt
https://tools.cisco.com/security/center/viewAlert.x?alertId=56774

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

Identifikátor

FFmpeg Denial of Service Vulnerability

Popis

Produkt FFmpeg obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol prostredníctvom špeciálneho podvrhnutého AVI súboru zneužiť na zneprístupnenie služby. Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov vo funkcii *decode_plane* definovanej v rámci súboru *libavcodec/utvideodec.c*.

Dátum prvého zverejnenia varovania

11.02.2018 (posledná aktualizácia 12.02.2018)

CVE

CVE-2018-6912

Zasiahnuté systémy

FFmpeg verzie 3.4.2, 3.3.6, 3.2.10, 3.1.11, 3.0.10

Následky

Zneprístupnenie služby

Odporúčania

Používateľom zasiahnutých produktov odporúčame bezodkladne vykonať ich aktualizáciu.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2018-6912
https://tools.cisco.com/security/center/viewAlert.x?alertId=56791

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

Identifikátor

F5 BIG-IP Policy Enforcement Manager URL Categorization Denial of Service Vulnerability

Popis

Spoločnosť F5 vydala bezpečnostnú aktualizáciu na svoj produkt BIG-IP, ktorá opravuje bezpečnostnú zraniteľnosť v Policy Enforcement Manager.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov v Traffic Management Microkernel a umožňuje vzdialenému útočníkovi pomocou podvrhnutia upravených URL adries spôsobiť pád systému a zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

06.02.2018

CVE

CVE-2017-6169

Zasiahnuté systémy

BIG-IP (PEM) verzie 11.6.0 až 11.6.2, 12.0.0 až 12.1.3 a 13.0.0

Následky

Zneprístupnenie služieb

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedeného produktu.

Zdroje

https://support.f5.com/csp/article/K31404801
https://tools.cisco.com/security/center/viewAlert.x?alertId=56690

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.1**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

PostgreSQL Denial of Service and Information Disclosure vulnerabilities

Popis

Vývojári databázového systému PostgreSQL vydali aktualizáciu svojho produktu, ktorá rieši viacero chýb a bezpečnostné zraniteľnosti spôsobené nesprávnym spracovaním citlivých údajov. Bezpečnostné zraniteľnosti umožňujú vzdialenému autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov spôsobiť zneprístupnenie služieb na zasiahnutom systéme a tiež získať prístup k citlivým informáciám.

Dátum prvého zverejnenia varovania

08.02.2018

CVE

CVE-2018-1052, CVE-2018-1053

Zasiahnuté systémy

PostgreSQL verzie 10.0.0, 10.1.0

Následky

Zneprístupnenie služieb, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedeného produktu.

Zdroje

https://www.postgresql.org/docs/current/static/release-10-2.html
http://www.vuxml.org/freebsd/c602c791-0cf4-11e8-a2ec-6cc21735f730.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=56762
https://tools.cisco.com/security/center/viewAlert.x?alertId=56763

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.5**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Brocade Fabric OS Multiple Vulnerabilities

Popis

Webové manažmentové rozhranie Brocade Fabric OS obsahuje zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku a v prípade jeho úspešnosti vykonať škodlivý kód. Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov.

IPv6 stack Brocade Fabric OS obsahuje zraniteľnosť, ktorú by lokálny neautentifikovaný útočník mohol zneužiť na znepristupnenie služieb. Zraniteľnosť spočíva v nesprávnom spracovávaní RA (Router Advertisement) správ.

Dátum prvého zverejnenia varovania

09.02.2018

CVE

CVE-2017-6225, CVE-2017-6227

Zasiahnuté systémy

Brocade Fabric OS 7.4.0, 7.4.1, 7.4.2, 8.1.0, 8.1.1

Následky

Znepristupnenie služby, Vykonanie škodlivého kódu

Odporúčania

Spoločnosť Brocade vydala bezpečnostnú aktualizáciu riešiacu uvedené zraniteľnosti. Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=56771
https://tools.cisco.com/security/center/viewAlert.x?alertId=56772

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.1**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Cisco Data Center Analytics Cross-Site Scripting Vulnerabilities

Popis

Webové manažmentové rozhranie produktu Cisco Data Center Analytics Framework obsahuje zraniteľnosti, ktoré by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie XSS (Cross-Site Scripting) útoku.
Zraniteľnosť spočíva v nedostatočnom overovaním používateľských vstupov. Úspešným XSS útokom by útočník mohol získať prístup k citlivým údajom, ktoré by mohol zneužiť na prípravu nadväzujúcich útokov.

Dátum prvého zverejnenia varovania

07.02.2018

CVE

CVE-2018-0128, CVE-2018-0129

Zasiahnuté systémy

Cisco Data Center Analytics Framework

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180207-dcaf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180207-dcaf1