# BEZPEČNOSTNÝ BULLETIN

Týždeň 17. 01. 2018 – 23. 01. 2018

## OBSAH BEZPEČNOSTNÉHO BULLETINU

| Číslo | Identifikátor | Dôležitosť | CVSS Skóre |
|---|---|---|---|
| **1** | Enterprise Networking Operating System (ENOS) Authentication Bypass vulnerability | Vysoká | **7.8** |
| **2** | ISC BIND Improper fetch cleanup vulnerability | Vysoká | **7.5** |
| **3** | WordPress 4.9.2 Security and Maintenance Release | Vysoká | **7.5** |
| **4** | Cisco NX-OS Software Multiple Vulnerabilities | Vysoká | **7.4** |
| **5** | Glibc Underflow Local Code Execution Vulnerability | Vysoká | **7.0** |
| **6** | Cisco WebEx Meetings Server Multiple Vulnerabilities | Stredná | **6.4** |
| **7** | F5 Networks BIG-IP (AFM) Vulnerability | Stredná | **5.4** |

**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:
00099/2018/SKB/OBPr-050

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 7.8** |
| **Klasifikácia** | ☒ **Neutajované / TLP (WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Enterprise Networking Operating System (ENOS) Authentication Bypass vulnerability

## Popis

Viaceré switche výrobcov Lenovo a IBM obsahujú zraniteľnosť známu ako „HP Backdoor“. Ide o nezdokumentované "zadné dvierka" vo firmvéri Enterprise Networking Operating System (ENOS) - spôsob, ako za určitých okolností obísť autentifikáciu a získať administrátorský prístup na dotknutý switch.
To môže viesť k úniku informácií o sieťových nastaveniach, umožniť útočníkovi v lokálnej sieti neoprávnený prístup k dátam z iných sieťových segmentov, prípadne rekonfiguráciou sieťových nastavení spôsobiť nedostupnosť sieťovej komunikácie.

## Dátum prvého zverejnenia varovania

11.01.2018

## CVE

CVE-2017-3765

## Zasiahnuté systémy

Lenovo Flex Switch, Lenovo RackSwitch, IBM Flex System Switch, IBM BladeCenter, IBM RackSwitch

## Následky

Odopretie služieb, Narušenie dôvernosti a integrity sieťovej komunikácie

## Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedeného produktu.

## Zdroje

https://support.lenovo.com/sk/en/product_security/len-16095

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

## Identifikátor

ISC BIND Improper fetch cleanup vulnerability

## Popis

Bezpečnostná zraniteľnosť v ISC BIND umožňuje vzdialenému útočníkovi pomocou podvrhnutých DNS požiadaviek spôsobiť pád aplikácie a odopretie služieb. Zraniteľnosť nachádzajúca sa v knižnici *netaddr.c* je spôsobená nesprávnym overovaním používateľských vstupov.

## Dátum prvého zverejnenia varovania

16.01.2018

## CVE

CVE-2017-3145

## Zasiahnuté systémy

BIND 9.0.0 až 9.8.x, 9.9.0 až 9.9.11, 9.10.0 až 9.10.6, 9.11.0 až 9.11.2, 9.9.3-S1 až 9.9.11-S1, 9.10.5-S1 až 9.10.6-S1, 9.12.0a1 až 9.12.0rc1

## Následky

Odopretie služieb

## Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedeného produktu.

## Zdroje

https://www.securitytracker.com/id/1040195
https://kb.isc.org/article/AA-01542
https://www.theregister.co.uk/2018/01/17/bind_patch_catches_crashes/
https://bugzilla.redhat.com/show_bug.cgi?id=1534812

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

## Identifikátor

WordPress 4.9.2 Security and Maintenance Release

## Popis

Bola vydaná aktualizácia WordPress 4.9.2, ktorá odstraňuje viacero chýb a bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť v *wp-includes/js/mediaelement* umožňuje vzdialenému útočníkovi použiť XSS (Cross-Site Scripting) útok a vykonať škodlivý kód.

## Dátum prvého zverejnenia varovania

16.01.2018

## CVE

CVE-2018-5776

## Zasiahnuté systémy

WordPress verzie nižšie ako 4.9.2.

## Následky

Vykonanie škodlivého kódu

## Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedeného produktu.

## Zdroje

https://wordpress.org/news/2018/01/wordpress-4-9-2-security-and-maintenance-release/
https://github.com/WordPress/WordPress/commit/3fe9cb61ee71fcfadb5e002399296fcc1198d850
https://nvd.nist.gov/vuln/detail/CVE-2018-5776

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 7.4** |
| **Klasifikácia** | ☒ **TLP (WHITE)** | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** | |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Cisco NX-OS Software Multiple Vulnerabilities

## Popis

Produkt Cisco NX-OS Software obsahuje viacero zraniteľností, ktoré by útočník mohol zneužiť na odopretie služieb.
Prvá sa nachádza v nástroji Pong, ktorý počas svojej činnosti 2 krát uvoľňuje rovnakú časť pamäte a možno ju zneužiť na reštartovanie supervízora vPC (Virtual Port-Channel). Zraniteľnosť možno zneužiť len v prípade, že je na dotknutom zariadení aktivovaný nástroj Pong, funkcia FabricPath a SPAN (Switched Port Analyzer) vykonáva aktívne monitorovanie FabricPath portu.
Zraniteľnosť v manažmentovom rozhraní na konfiguráciu ACL (Access Control List) by vzdialený neautentifikovaný útočník mohol zneužiť na obídenie pravidiel ACL, zahltenie NX-OS procesora a následné odopretie služieb.
Nesprávna implementácia role "network operator" umožňuje lokálnemu autentifikovanému útočníkovi vymazať existujúce používateľské kontá.

## Dátum prvého zverejnenia varovania

17.01.2018

## CVE

CVE-2018-0090, CVE-2018-0092, CVE-2018-0102

## Zasiahnuté systémy

Cisco NX-OS System Software

## Následky

Odopretie služieb

## Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutého produktu.

## Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180117-nx-os
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180117-nxos1
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180117-nxos

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 7.0** |
| **Klasifikácia** | ☒ **TLP (WHITE)** | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** | |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Glibc Underflow Local Code Execution Vulnerability

## Popis

Bezpečnostná zraniteľnosť v GNU Glibc umožňuje lokálnemu útočníkovi vyvolať pretečenie zásobníka a následne vykonať škodlivý kód a eskalovať svoje privilégiá v danom systéme. Zraniteľnosť sa nachádza vo funkcii *__realpath()* v súčasti *stdlib/canonicalize.c* a je spôsobená nesprávnym spracovaním adries vo funkcii *getcwd()*.

## Dátum prvého zverejnenia varovania

12.01.2018

## CVE

CVE-2018-1000001

## Zasiahnuté systémy

GNU Glibc

## Následky

Vykonanie škodlivého kódu, Eskalácia privilégií

## Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedeného produktu.

## Zdroje

https://sourceware.org/git/gitweb.cgi?p=glibc.git;h=52a713fdd0a30e1bd79818e2e3c4ab44ddca1a94
https://tools.cisco.com/security/center/viewAlert.x?alertId=56466

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☒ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 6.4** |
| **Klasifikácia** | ☒ **TLP (WHITE)** | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** | |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Cisco WebEx Meetings Server Multiple Vulnerabilities

## Popis

Produkt Cisco WebEx Meeting Server obsahuje viacero zraniteľností, ktoré možno zneužiť na získanie prístupu k citlivým údajom.
Zraniteľnosť umožňujúcu vykonávanie XXE (XML External Entity) injekcie by vzdialený neautentifikovaný útočník mohol zneužiť na odchytávanie a presmerovávanie súborov zákazníkov.
Ďalšie zraniteľnosti umožňujú vzdialenému autentifikovanému útočníkovi získať prístup k citlivým dátam aplikácie a k vzdialenému účtu technickej podpory (aj keď bol vypnutý prostredníctvom webového rozhrania).

## Dátum prvého zverejnenia varovania

17.01.2018

## CVE

CVE-2018-0108, CVE-2018-0109, CVE-2018-0110, CVE-2018-0111

## Zasiahnuté systémy

Cisco WebEx Meetings Server

## Následky

Prístup k citlivým údajom

## Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat bezodkladne vykonať aktualizáciu.

## Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180117-wms
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180117-wms1
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180117-wms2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180117-wms3

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☒ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 5.4** |
| **Klasifikácia** | ☒ **TLP (WHITE)** | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** | |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

F5 Networks BIG-IP (AFM) Vulnerability

## Popis

Spoločnosť F5 Networks vydala aktualizáciu na svoj produkt BIG-IP, ktorá rieši zraniteľnosť spočívajúcu v nesprávnom overovaní X509 certifikátov vo firewallovom module. Bezpečnostná zraniteľnosť umožňuje vzdialenému útočníkovi obísť overovanie identity vzdialených serverov a prostredníctvom man-in-the-middle útoku získať a modifikovať dáta posielané medzi vzdialeným serverom a napadnutým systémom.

## Dátum prvého zverejnenia varovania

18.01.2018

## CVE

CVE-2017-6142

## Zasiahnuté systémy

BIG-IP (AFM) 11.6.1, 11.6.2, 12.1.0 - 12.1.2, 13.0.0

## Následky

Prístup k citlivým údajom

## Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedeného produktu.

## Zdroje

https://support.f5.com/csp/article/K20682450
https://tools.cisco.com/security/center/viewAlert.x?alertId=56510