# BEZPEČNOSTNÝ BULLETIN

Týždeň 16. 01. 2019 - 22. 01. 2019

## OBSAH BEZPEČNOSTNÉHO BULLETINU

| Č. | Identifikátor | Dôležitosť | CVSS Skóre |
|---|---|---|---|
| **01.** | LCDS LAquis SCADA zraniteľnosti | Vysoká | **7.8** |
| **02.** | Check Point ZoneAlarm Zraniteľnosť | Vysoká | **7.8** |
| **03.** | ControlByWeb X-320M zraniteľnosť | Vysoká | **7.6** |
| **04.** | Scapy zraniteľnosť | Vysoká | **7.5** |
| **05.** | Drupal zraniteľnosti | Vysoká | **7.5** |
| **06.** | CoreOS etcd zraniteľnosť | Vysoká | **7.4** |
| **07.** | Omron CX-Supervisor zraniteľnosť | Vysoká | **7.3** |
| **08.** | ABB CP400 Panel Builder TextEditor 2.0 zraniteľnosť | Vysoká | **7.0** |
| **09.** | NTPsec zraniteľnosti | Stredná | **6.5** |

**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:
01380/2019/TS/OKB-022

# BEZPEČNOSTNÝ BULLETIN

Týždeň 16. 01. 2019 - 22. 01. 2019

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

## Identifikátor

LCDS LAquis SCADA zraniteľnosti

## Popis

Spoločnosť LCDS vydala bezpečnostnú aktualizáciu na svoj produkt LAquis SCADA, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

15.01.2019

## CVE

CVE-2018-18986, CVE-2018-18988, CVE-2018-18990, CVE-2018-18992, CVE-2018-18994, CVE-2018-18996, CVE-2018-18998, CVE-2018-19000, CVE-2018-19002, CVE-2018-19004, CVE-2018-19029

## Zasiahnuté systémy

LAquis SCADA verzie staršie ako 4.1.0.4150

## Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

## Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-015-01

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

## Identifikátor

Check Point ZoneAlarm Zraniteľnosť

## Popis

Spoločnosť Check Point vydala bezpečnostné aktualizácie, ktoré opravujú zraniteľnosť v produkte ZoneAlarm.
Bezpečnostná zraniteľnosť je spôsobená bližšie nešpecifikovanou chybou v komponente SBACipollaSrvHost a lokálny autentifikovaný útočník by ju mohol zneužiť na eskaláciu privilégií a následné vykonanie škodlivého kódu s privilégiami SYSTEM.
Na uvedenú zraniteľnosť je voľne dostupný Proof-Of-Concept kód.

## Dátum prvého zverejnenia varovania

17.01.2019

## CVE

-

## Zasiahnuté systémy

Check Point ZoneAlarm Free Antivirus + Firewall verzie 8.8.1.110

## Následky

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

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/155876

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 7.6 |
| **Klasifikácia** | ☒ **Neutajované / TLP(WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

ControlByWeb X-320M zraniteľnosť

## Popis

Spoločnosť ControlByWeb vydala bezpečnostnú aktualizáciu na meteorologickú stanicu X-320M, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému autentifikovanému útočníkovi vykonať škodlivý kód na napadnutom systéme.

## Dátum prvého zverejnenia varovania

17.01.2019

## CVE

CVE-2018-18881, CVE-2018-18882

## Zasiahnuté systémy

ControlByWeb X-320M verzie staršie ako 1.06

## Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-017-03

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

## Identifikátor

Scapy zraniteľnosť

## Popis

Vývojári analyzátora paketov Scapy vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov zasiahnutým systémom a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených Radius paketov spôsobiť zneprístupnenie služieb.

## Dátum prvého zverejnenia varovania

08.01.2019

## CVE

-

## Zasiahnuté systémy

Scapy verzia 2.4.0 a staršie

## Následky

Zneprístupnenie služby

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://www.imperva.com/blog/scapy-sploit-python-network-tool-is-vulnerable-to-denial-of-service-dos-attack-cve-pending/
https://www.securityweek.com/dos-vulnerability-found-scapy-packet-manipulation-tool

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

## Identifikátor

Drupal zraniteľnosti

## Popis

Vývojári redakčného systému Drupal vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov zasiahnutým systémom a umožňuje vzdialenému autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených požiadaviek vykonať škodlivý kód.

## Dátum prvého zverejnenia varovania

16.01.2019

## CVE

CVE-2018-1000888

## Zasiahnuté systémy

Drupal verzie staršie ako 8.6.6; 8.5.9 a 7.62

## Následky

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

## Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Drupal v zraniteľných verziách. V prípade že áno, zabezpečte aktualizáciu redakčného systému a pluginov.

## Zdroje

https://www.drupal.org/sa-core-2019-001
https://www.drupal.org/sa-core-2019-002
https://exchange.xforce.ibmcloud.com/vulnerabilities/155668

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

## Identifikátor

CoreOS etcd zraniteľnosť

## Popis

Vývojári nástroja CoreOS Etcd vydali aktualizáciu svojho produktu, ktorá rieši bezpečnostnú zraniteľnosť spôsobenú nedostatočným overovaním certifikátov.
Bezpečnostná zraniteľnosť umožňuje vzdialenému autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených požiadaviek získať neoprávnený prístup do systému.

## Dátum prvého zverejnenia varovania

11.01.2019

## CVE

CVE-2018-16886

## Zasiahnuté systémy

CoreOS etcd verzie staršie ako 3.3.26 a 3.3.11

## Následky

Neoprávnený prístup do systému

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59474
https://access.redhat.com/security/cve/cve-2018-16886

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 7.3** |
| **Klasifikácia** | ☒ **Neutajované / TLP(WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Omron CX-Supervisor zraniteľnosť

## Popis

Spoločnosť Omron vydala bezpečnostnú aktualizáciu na svoj produkt CX-Supervisor, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nesprávnym spracovaním projektových súborov a umožňujú lokálnemu autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených projektových súborov vykonať škodlivý kód.

## Dátum prvého zverejnenia varovania

17.01.2019

## CVE

CVE-2018-19011, CVE-2018-19013, CVE-2018-19015, CVE-2018-19017, CVE-2018-19019

## Zasiahnuté systémy

CX-Supervisor verzie staršie ako 3.5.0.11

## Následky

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

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-017-01

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

## Identifikátor

ABB CP400 Panel Builder TextEditor 2.0 zraniteľnosť

## Popis

Spoločnosť ABB vydala bezpečnostnú aktualizáciu na svoj produkt CP400PB, ktorá opravuje bezpečnostnú zraniteľnosť v textovom editore.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód.

## Dátum prvého zverejnenia varovania

17.01.2019

## CVE

CVE-2018-19008

## Zasiahnuté systémy

ABB CP400PB, Panel Builder pre CP405 a CP408 verzie staršie ako 2.1.7.21

## Následky

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

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-017-02

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

## Identifikátor

NTPsec zraniteľnosti

## Popis

Vývojári produktu NTPsec vydali aktualizáciu, ktorá rieši viacero chýb a bezpečnostných zraniteľností. 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

15.01.2019

## CVE

CVE-2019-6442, CVE-2019-6443, CVE-2019-6444, CVE-2019-6445

## Zasiahnuté systémy

ntpsec verzie staršie ako 1.1.3

## Následky

Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://dumpco.re/blog/ntpsec-bugs
https://dumpco.re/bugs/ntpsec-authed-oobwrite
https://dumpco.re/bugs/ntpsec-authed-npe
https://dumpco.re/bugs/ntpsec-oobread2
https://dumpco.re/bugs/ntpsec-oobread1