# BEZPEČNOSTNÝ BULLETIN

Týždeň 03. 07. 2019 - 09. 07. 2019

## OBSAH BEZPEČNOSTNÉHO BULLETINU

| Č. | Identifikátor | Dôležitosť | CVSS Skóre |
|---|---|---|---|
| **01.** | Cisco produkty viacero zraniteľností | Vysoká | **8.6** |
| **02.** | Foxit Software Foxit Reader a Foxit PhantomPDF zraniteľnosti | Vysoká | **7.8** |
| **03.** | Zipato ZipaMicro a Zipabox zraniteľnosti | Vysoká | **7.5** |
| **04.** | Schneider Electric Modicon Controllers zraniteľnosť | Vysoká | **7.5** |
| **05.** | GNOME libcroco zraniteľnosti | Stredná | **6.5** |
| **06.** | OzLabs Patchwork zraniteľnosť | 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 2915

**SK-CERT**
Naša značka:
01380/2019/TS/OKB-180

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 8.6** |
| **Klasifikácia** | ☒ **Neutajované / TLP(WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Cisco produkty viacero zraniteľností

## Popis

Spoločnosť Cisco vydala aktualizácie na väčšie množstvo svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť v produkte Unified Communications Manager je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom špeciálne upravených SIP paketov spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

03.07.2019

## CVE

CVE-2019-1884, CVE-2019-1886, CVE-2019-1887, CVE-2019-1889, CVE-2019-1890, CVE-2019-1891, CVE-2019-1892, CVE-2019-1893, CVE-2019-1894, CVE-2019-1906, CVE-2019-1909, CVE-2019-1911, CVE-2019-1921, CVE-2019-1922, CVE-2019-1930, CVE-2019-1931, CVE-2019-1932, CVE-2019-1933

## Zasiahnuté systémy

Cisco Unified Communications Manager
Cisco Web Security Appliance
Cisco IP Phone 7800 and 8800 Series
Cisco IOS XR Software Border Gateway Protocol
Cisco Firepower Management Center
Cisco Email Security Appliance
Cisco Unified Communications Domain Manager
Cisco Advanced Malware Protection
Cisco Prime Infrastructure and Evolved Programmable Network Manager
Cisco Small Business Series Switches
Cisco Enterprise NFV Infrastructure Software
Cisco Nexus 9000 Series Fabric Switches ACI Mode Fabric Infrastructure
Cisco Jabber for Windows
Cisco Application Policy Infrastructure Controller

## Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií
Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému
Neoprávnená zmena v systéme
Zneprístupnenie služby

| **Odporúčania** |
| --- |
| Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.<br>Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).<br>Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč. |

| **Zdroje** |
| --- |
| https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-wsa-dos<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-sbss-memcorrupt<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-sbss-dos<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-nfvis-file-readwrite<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-nfvis-commandinj<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-n9kaci-bypass<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-jabber-dll<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-cucm-dos<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-ccapic-restapi<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-asyncos-wsa<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-ip-phone-sip-dos<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-iosxr-bgp-dos<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-fmc-xss<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-esa-filterpass<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-esa-bypass<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-cucdm-rsh<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-amp-commandinj<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190619-prime-privescal |

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

## Identifikátor

Foxit Software Foxit Reader a Foxit PhantomPDF zraniteľnosti

## Popis

Spoločnosť Foxit Software vydala bezpečnostnú aktualizáciu na svoje produkty Foxit Reader a Foxit PhantomPDF, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

04.07.2019

## CVE

CVE-2019-13315, CVE-2019-13316, CVE-2019-13317, CVE-2019-13318, CVE-2019-13319, CVE-2019-13320, CVE-2019-6774, CVE-2019-6775, CVE-2019-6776

## Zasiahnuté systémy

Foxit Reader verzie staršie ako 9.6
Foxit PhantomPDF verzie staršie ako 9.6

## Následky

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

## Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

## Zdroje

https://www.foxitsoftware.com/support/security-bulletins.php
https://exchange.xforce.ibmcloud.com/vulnerabilities/163434
https://exchange.xforce.ibmcloud.com/vulnerabilities/163433
https://exchange.xforce.ibmcloud.com/vulnerabilities/163432
https://exchange.xforce.ibmcloud.com/vulnerabilities/163431
https://exchange.xforce.ibmcloud.com/vulnerabilities/163430
https://exchange.xforce.ibmcloud.com/vulnerabilities/163429
https://exchange.xforce.ibmcloud.com/vulnerabilities/163428
https://exchange.xforce.ibmcloud.com/vulnerabilities/163427
https://exchange.xforce.ibmcloud.com/vulnerabilities/163426

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

## Identifikátor

Zipato ZipaMicro a Zipabox zraniteľnosti

## Popis

Spoločnosť Zipato vydala bezpečnostné aktualizácie na svoje ovládače smart domácností Z-Wave Controller, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom. Zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente získať úplnú kontrolu nad systémom.
Proof-of-concept (PoC) kód je v súčasnosti verejne dostupný.

## Dátum prvého zverejnenia varovania

02.07.2019

## CVE

CVE-2019-9560, CVE-2019-9561, CVE-2019-9562

## Zasiahnuté systémy

ZipaMicro Z-Wave Controller Model verzia ZM.ZWUS
Zipabox Z-Wave Controller Model verzia 2AAU7-ZBZWUS

## Následky

Neoprávnený prístup do systému
Neoprávnená zmena v systéme

## Odporúčania

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

## Zdroje

https://siliconangle.com/2019/07/02/vulnerabilities-zipato-smart-home-devices-let-hackers-open-doors/
https://blackmarble.sh/zipato-smart-hub/
https://nakedsecurity.sophos.com/2019/07/04/open-sesame-zipatos-smart-hub-hacked-to-open-front-doors/

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

## Identifikátor

Schneider Electric Modicon Controllers zraniteľnosť

## Popis

Spoločnosť Schneider Electric vydala bezpečnostné aktualizácie na svoje automatizačné ovládače Modicon M340 a M580, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom špeciálne vytvoreného Modbus súboru spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

02.07.2019

## CVE

CVE-2019-6819

## Zasiahnuté systémy

Modicon M340 verzie staršie ako 3.01
Modicon M580 verzie staršie ako 2.80
Modicon Quantum všetky verzie
Modicon Premium všetky verzie

## Následky

Zneprístupnenie služby

## Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

## Zdroje

https://www.us-cert.gov/ics/advisories/icsa-19-183-01
https://nvd.nist.gov/vuln/detail/CVE-2019-6819

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

## Identifikátor

GNOME libcroco zraniteľnosti

## Popis

Spoločnosť GNOME Project vydala bezpečnostné aktualizácie na svoj syntaktický analyzátor libcroco, ktoré opravujú bezpečnostné zraniteľnosti vo funkciách r_tknzr_parse_comment a cr_parser_parse_selector_core.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

05.07.2019

## CVE

CVE-2017-8834, CVE-2017-8871

## Zasiahnuté systémy

GNOME libcroco verzia 0.6 (.12)

## Následky

Zneprístupnenie služby

## Odporúčania

Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

## Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=60384
https://tools.cisco.com/security/center/viewAlert.x?alertId=60385
https://bugzilla.gnome.org/show_bug.cgi?id=782647
https://bugzilla.gnome.org/show_bug.cgi?id=782649

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

## Identifikátor

OzLabs Patchwork zraniteľnosť

## Popis

Vývojári produktu OzLabs Patchwork vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť Message-ID pola.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webstránky získať prístup k citlivým údajom.

## Dátum prvého zverejnenia varovania

05.07.2019

## CVE

CVE-2019-13122

## Zasiahnuté systémy

OzLabs Patchwork verzie staršie ako 2.0.4
OzLabs Patchwork verzie staršie ako 2.1.4

## Následky

Neoprávnený prístup k citlivým údajom

## Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

## Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/163451
https://seclists.org/oss-sec/2019/q3/7