# BEZPEČNOSTNÝ BULLETIN

Týždeň 16. 10. 2019 - 22. 10. 2019

## OBSAH BEZPEČNOSTNÉHO BULLETINU



**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/SK-CERT-255

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

## Identifikátor

Jenkins plugins viacero zraniteľností

## Popis

Vývojári produktu Jenkins informovali o bezpečnostných zraniteľnostiach vo viacerých zásuvných moduloch.
Najvážnejšia bezpečnostná zraniteľnosť v Puppet Enterprise Pipeline Plugin je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

16.10.2019

## CVE

CVE-2019-10436, CVE-2019-10437, CVE-2019-10438, CVE-2019-10439, CVE-2019-10440, CVE-2019-10441, CVE-2019-10442, CVE-2019-10443, CVE-2019-10444, CVE-2019-10445, CVE-2019-10446, CVE-2019-10447, CVE-2019-10448, CVE-2019-10449, CVE-2019-10450, CVE-2019-10451, CVE-2019-10452, CVE-2019-10453, CVE-2019-10454, CVE-2019-10455, CVE-2019-10456, CVE-2019-10457, CVE-2019-10458

## Zasiahnuté systémy

Bumblebee HP ALM Plugin verzie staršie ako 4.1.4
Cadence vManager Plugin verzie staršie ako 2.7.0
CRX Content Package Deployer Plugin verzie staršie ako 1.8.1
Delphix Plugin 2.0.4 a staršie
ElasticBox CI Plugin 5.0.1 a staršie
Extensive Testing Plugin 1.4.4b a staršie
Fortify on Demand Plugin 4.0.0 a staršie
Google Kubernetes Engine Plugin verzie staršie ako 0.7.0
Google OAuth Credentials Plugin verzie staršie ako 0.9
iceScrum Plugin verzie staršie ako 1.1.5
NeoLoad Plugin verzie staršie ako 2.2.5
Oracle Cloud Infrastructure Compute Classic Plugin 1.0.0 a staršie
Puppet Enterprise Pipeline Plugin 1.3.1 a staršie
Rundeck Plugin 3.6.5 a staršie
SOASTA CloudTest Plugin 2.25 a staršie
Sofy.AI Plugin 1.0.3 a staršie
View26 Test-Reporting Plugin 1.0.7 a staršie

## Následky

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

| **Odporúčania** |
| --- |
| Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.<br>V prípade pluginov, na ktoré doposiaľ neboli vydané aktualizácie administrátorom odporúčame zvážiť ich odinštalovanie a tiež sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.<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://jenkins.io/security/advisory/2019-10-16/#SECURITY-1439 |

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

## Identifikátor

Linux Kernel rtlwifi zraniteľnosť

## Popis

Bezpečnostní výskumníci informovali o bezpečnostnej zraniteľnosti v ovládači rtlwifi v linuxovom jadre. Bezpečnostná zraniteľnosť v ovládači Realtek Wi-Fi chipov je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi, nachádzajúcemu sa v dosahu WiFi prijímača prostredníctvom zasielania špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

17.10.2019

## CVE

CVE-2019-17666

## Zasiahnuté systémy

Linux Kernel verzie 3.10.1 až 5.3.6

## Následky

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

## Odporúčania

Bezpečnostná aktualizácia riešiaca uvedenú zraniteľnosť doposiaľ nebola vydaná. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
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://gbhackers.com/wi-fi-vulnerability-in-linux/
https://nvd.nist.gov/vuln/detail/CVE-2019-17666
https://sensorstechforum.com/cve-2019-17666-linux-rtlwifi-driver/
https://arstechnica.com/information-technology/2019/10/unpatched-linux-flaw-may-let-attackers-crash-or-compromise-nearby-devices/

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 8.4** |
| **Klasifikácia** | ☒ **Neutajované / TLP(WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

IBM Workload Scheduler zraniteľnosť

## Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Workload Scheduler, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá a vykonávať neoprávnené zmeny v systéme.

## Dátum prvého zverejnenia varovania

09.10.2019

## CVE

CVE-2019-4031

## Zasiahnuté systémy

IBM Workload Scheduler verzie staršie ako 9.2.0-TIV-TWS-FP0003-IJ15085 a 9.3.0-TIV-TWS-FP0003-IJ15085

## Následky

Eskalácia privilégií
Neoprávnená zmena v systéme

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/155997
https://www.ibm.com/support/pages/node/1076775

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

## Identifikátor

Zraniteľnosť tlačiarní HP

## Popis

Spoločnosť HP vydala bezpečnostnú aktualizáciu na svoje tlačiarne HP LaserJet, PageWide a OfficeJet Enterprise, ktorá opravuje bezpečnostnú zraniteľnosť.
Bližšie nešpecifikovaná bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

12.10.2019

## CVE

CVE-2019-6334

## Zasiahnuté systémy

HP LaserJet
PageWide
OfficeJet Enterprise
LaserJet Managed Printers

## Následky

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

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://support.hp.com/us-en/document/c06447795

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

## Identifikátor

Horner Automation Cscape zraniteľnosti

## Popis

Spoločnosť Horner Automation vydala bezpečnostnú aktualizáciu na svoj produkt Cscape, ktorá opravuje bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti vo funkcii parsovania CSP súborov sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

17.10.2019

## CVE

CVE-2019-13541, CVE-2019-13545

## Zasiahnuté systémy

Horner Automation Cscape verzie staršie ako 9.90 SP1

## Následky

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

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

## Zdroje

https://www.us-cert.gov/ics/advisories/icsa-19-290-02
https://www.zerodayinitiative.com/advisories/ZDI-19-903/
https://www.zerodayinitiative.com/advisories/ZDI-19-902/

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

## Identifikátor

WordPress bezpečnostné zraniteľnosti

## Popis

Vývojári redakčného systému WordPress vydali aktualizáciu svojho produktu, ktorá rieši viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting útoku získať prístup k citlivým údajom.

## Dátum prvého zverejnenia varovania

14.10.2019

## CVE

CVE-2019-17669, CVE-2019-17670, CVE-2019-17671, CVE-2019-17672, CVE-2019-17673, CVE-2019-17674, CVE-2019-17675

## Zasiahnuté systémy

WordPress verzie staršie ako 5.2.4

## Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

## Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Wordpress v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu redakčného systému a všetkých pluginov. 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.

## Zdroje

https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/

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

## Identifikátor

AVEVA Vijeo Citect a Citect SCADA zraniteľnosť

## Popis

Spoločnosť Aveva vydala bezpečnostné aktualizácie na svoje produkty Vijeo Citect a Citect SCADA, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť v ovládači IEC870IP umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť pretečenie zásobníka a zneprístupnenie služieb.

## Dátum prvého zverejnenia varovania

15.10.2019

## CVE

CVE-2019-13537

## Zasiahnuté systémy

IEC870IP driver verzie staršie ako v4.15.00

## Následky

Zneprístupnenie služieb

## Odporúčania

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

## Zdroje

https://www.us-cert.gov/ics/advisories/icsa-19-290-01
https://sw.aveva.com/hubfs/assets-2018/pdf/security-bulletin/SecurityBulletin_LFSec139.pdf

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

## Identifikátor

Apache Thrift zraniteľnosti

## Popis

Vývojári systému Apache Thrift vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služieb.

## Dátum prvého zverejnenia varovania

14.10.2019

## CVE

CVE-2019-0205, CVE-2019-0210

## Zasiahnuté systémy

Apache Thrift verzie staršie ako 0.13.0

## Následky

Zneprístupnenie služby

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://seclists.org/oss-sec/2019/q4/28
https://seclists.org/oss-sec/2019/q4/29
https://exchange.xforce.ibmcloud.com/vulnerabilities/169460
https://exchange.xforce.ibmcloud.com/vulnerabilities/169459

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

## Identifikátor

Sangoma SBC zraniteľnosti

## Popis

Spoločnosť Sangoma vydala bezpečnostnú aktualizáciu na svoj produkt Sangoma SBC, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému.

## Dátum prvého zverejnenia varovania

17.10.2019

## CVE

CVE-2019-12147, CVE-2019-12148

## Zasiahnuté systémy

Sangoma SBC verzie staršie ako 2.3.24

## Následky

Neoprávnený prístup do systému

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Odporúčame tiež vykonať kontrolu systému na prítomnosť neoprávnených používateľských účtov.

## Zdroje

https://seclists.org/fulldisclosure/2019/Oct/41
https://seclists.org/fulldisclosure/2019/Oct/40
https://exchange.xforce.ibmcloud.com/vulnerabilities/169567
https://exchange.xforce.ibmcloud.com/vulnerabilities/169568