BEZPEČNOSTNÝ BULLETIN

Týždeň 20. 06. 2018 – 26. 06. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	TIBCO Data Virtualization Command Injection Vulnerability	Vysoká	**8.8**
02.	Rockwell Automation Allen-Bradley CompactLogix and GuardLogix Vulnerability	Vysoká	**8.6**
03.	phpMyAdmin Multiple Vulnerabilities	Vysoká	**8.1**
04.	Axis Cameras Multiple Vulnerabilities	Vysoká	**8.1**
05.	Micro Focus UCMDB Multiple Vulnerabilities	Vysoká	**7.5**
06.	QNAP QTS LDAP Server Vulnerability	Vysoká	**7.3**
07.	Delta Electronics Delta Industrial Automation COMMGR Vulnerability	Vysoká	**7.3**
08.	Symantec Endpoint Protection Multiple Vulnerabilities	Stredná	**6.5**
09.	Apache Qpid Broker-J Denial of Service Vulnerability	Stredná	**6.5**
10.	SAJ Solar Inverter Information Disclosure Vulnerability	Stredná	**5.3**

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:
02049/2018/TS/OKB-080

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

Identifikátor

TIBCO Data Virtualization Command Injection Vulnerability

Popis

Spoločnosť TIBCO vydala bezpečnostnú aktualizáciu na svoj produkt Data Virtualization. Bližšie nešpecifikovanú bezpečnostnú zraniteľnosť v komponente Version Control Adapters by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených požiadaviek mohol zneužiť na vykonanie škodlivého kódu v kontexte používateľa Data Virtualization servera.

Dátum prvého zverejnenia varovania

20.06.2018

CVE

CVE-2018-5428

Zasiahnuté systémy

TIBCO Data Virtualization verzie 7.0.5, 7.0.6

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.tibco.com/support/advisories/2018/06/tibco-security-advisory-june-20-2018-tibco-data-virtualization

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

Identifikátor

Rockwell Automation Allen-Bradley CompactLogix and GuardLogix Vulnerability

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu na svoje produkty Allen-Bradley CompactLogix a Compact GuardLogix, ktorá opravuje bližšie nešpecifikovanú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému útočníkovi prostredníctvom zasielania špeciálne upravených TCP paketov spôsobiť chybu Major Non-Recoverable Fault (MNRF) a následné zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

21.06.2018

CVE

CVE-2017-9312

Zasiahnuté systémy

Allen-Bradley CompactLogix 5370 L1 controllers, verzie staršie ako 31.011
Allen-Bradley CompactLogix 5370 L2 controllers, verzie staršie ako 31.011
Allen-Bradley CompactLogix 5370 L3 controllers, verzie staršie ako 31.011
Allen-Bradley Armor CompactLogix 5370 L3 controllers, verzie staršie ako 31.011
Allen-Bradley Compact GuardLogix 5370 controllers, verzie staršie ako 31.011
Allen-Bradley Armor Compact GuardLogix 5370 controllers, verzie staršie ako 31.011

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). Tiež odporúčame blokovať porty 2222/TCP a UDP a 44818/TCP a UDP.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-172-02
https://www.securityweek.com/rockwell-patches-flaw-affecting-safety-controllers-several-vendors

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

Identifikátor

phpMyAdmin Multiple Vulnerabilities

Popis

Vývojári phpMyAdmin vydali aktualizácie svojho produktu, ktoré opravujú viacero bezpečnostných zraniteľností.
Prvá zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov v komponente Designer a vzdialený neautentifikovaný útočník by ju mohol zneužiť na realizáciu XSS (Cross Site Scripting) útoku, vykonanie škodlivého kódu a získanie prístupu k údajom uloženým v cookies, vrátane autentifikačných údajov.
Druhá zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a vzdialený autentifikovaný útočník by ju mohol zneužiť na nahratie súborov na webový server a potenciálne vykonanie škodlivého kódu. Uvedenú zraniteľnosť je možné zneužiť aj bez potreby autentifikácie, pri nasledujúcej konfigurácii:

```
$cfg['AllowArbitraryServer'] = true;
$cfg['ServerDefault'] = 0;
```

Dátum prvého zverejnenia varovania

19.06.2018 (posledná aktualizácia 21.06.2018)

CVE

CVE-2018-12581, CVE-2018-12613

Zasiahnuté systémy

phpMyAdmin verzie staršie ako 4.8.2 (CVE-2018-12581)
phpMyAdmin verzie 4.8.0, 4.8.1 (CVE-2018-12613)

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.phpmyadmin.net/security/PMASA-2018-3/
https://www.phpmyadmin.net/security/PMASA-2018-4/

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

Identifikátor

Axis Cameras Multiple Vulnerabilities

Popis

Spoločnosť Axis Communications AB vydala bezpečnostné aktualizácie na 392 modelov bezpečnostných kamier, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšie bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému útočníkovi získať neoprávnený prístup do napadnutého zariadenia, modifikovať jeho nastavenia a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.06.2018

CVE

CVE-2018-10658, CVE-2018-10659, CVE-2018-10660, CVE-2018-10661, CVE-2018-10662, CVE-2018-10663, CVE-2018-10664

Zasiahnuté systémy

Kompletný zoznam zasiahnutých produktov nájdete na nasledujúcom odkaze:
https://www.axis.com/files/sales/ACV-128401_Affected_Product_List.pdf

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov a aplikovať firewallové pravidlá s blokovaním portov 80 a 443, prostredníctvom ktorých je vykonávaná konfigurácia daných zariadení.

Zdroje

https://blog.vdoo.com/2018/06/18/vdoo-discovers-significant-vulnerabilities-in-axis-cameras/
https://www.bleepingcomputer.com/news/security/vendor-patches-seven-vulnerabilities-across-392-camera-models/

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

Identifikátor

Micro Focus UCMDB Multiple Vulnerabilities

Popis

Spoločnosť Micro Focus vydala bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností v produkte Universal Configuration Management Database Browser (UCMDB).
Bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník mohol prostredníctvom CSRF (Cross-Site Request Forgery) útoku zneužiť na vykonanie príkazov v kontexte prihláseného používateľa.
Uvedené zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť aj na útok typu Java Object Deserialization. Spoločnosť Micro Focus bližšie nešpecifikuje následky tohto typu útoku.

Dátum prvého zverejnenia varovania

15.06.2018 (posledná aktualizácia 19.06.2018)

CVE

CVE-2018-6496, CVE-2018-6497

Zasiahnuté systémy

UCMDB Browser verzie 4.10, 4.11, 4.12, 4.13, 4.14, 4.15, 4.15.1
Universal CMDB Server; DDM Content Pack verzie 10.20, 10.21, 10.22, 10.22 CUP7, 10.30, 10.31, 10.32, 10.33, 10.33 CUP2, 11.0, CMS Server 2018.05

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://softwaresupport.softwaregrp.com/document/facetsearch/document/KM03180066
https://softwaresupport.softwaregrp.com/document/facetsearch/document/KM03180069
https://www.securitytracker.com/id/1041139
https://www.securitytracker.com/id/1041140

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

Identifikátor

QNAP QTS LDAP Server Vulnerability

Popis

Spoločnosť QNAP vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v produkte QTS.
Bližšie nešpecifikovanú zraniteľnosť v komponente LDAP Server by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie systémových príkazov a škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.06.2018

CVE

CVE-2018-0712

Zasiahnuté systémy

LDAP server v QTS 4.2.6: build 20171208 a staršie verzie
LDAP server v QTS 4.3.3: build 20180402 a staršie verzie
LDAP server v QTS 4.3.4: build 20180413 a staršie verzie

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.qnap.com/zh-tw/security-advisory/nas-201806-19
https://exchange.xforce.ibmcloud.com/vulnerabilities/145181

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

Identifikátor

Delta Electronics Delta Industrial Automation COMMGR Vulnerability

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na svoj produkt Delta Industrial Automation COMMGR, ktorá opravuje bližšie nešpecifikovanú bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a vzdialený útočník by ju prostredníctvom podvrhnutia špeciálne upravených paketov mohol zneužiť na vykonanie škodlivého kódu alebo zneprístupnenie služby.

Dátum prvého zverejnenia varovania

21.06.2018

CVE

CVE-2018-10594

Zasiahnuté systémy

Delta Industrial Automation COMMGR verzie staršie ako 1.09
DVPSimulator EH2, EH3, ES2, SE, SS2
AHSIM_5x0, AHSIM_5x1

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a povoliť prístup k portom 502 a 10002 iba pre vybrané aplikácie.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-172-01

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

Identifikátor

Symantec Endpoint Protection Multiple Vulnerabilities

Popis

Spoločnosť Symantec vydala bezpečnostné aktualizácie pre svoj produkt Endpoint Protection, ktoré opravujú viacero bezpečnostných zraniteľností.
Prvú zraniteľnosť by lokálny autentifikovaný útočník mohol zneužiť na vyvolanie stavu race condition a následné zneprístupnenie služby.
Druhú zraniteľnosť by lokálny autentifikovaný útočník mohol zneužiť na eskaláciu privilégií v systéme.

Dátum prvého zverejnenia varovania

21.06.2018

CVE

CVE-2018-5236, CVE-2018-5237

Zasiahnuté systémy

Symantec Endpoint Protection verzie staršie ako 14 RU1 MP1 alebo 12.1 RU6 MP10

Následky

Zneprístupnenie služby, Eskalácia privilégií

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.symantec.com/en_US/article.SYMSA1454.html

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

Identifikátor

Apache Qpid Broker-J Denial of Service Vulnerability

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v produkte Qpid Broker-J.
Bezpečnostná zraniteľnosť spočíva v implementačnej chybe, ktorú by vzdialený útočník prostredníctvom podvrhnutia správ presahujúcich limit maximálnej veľkosti správ (100MB) mohol zneužiť na zneprístupnenie služby. Uvedenú zraniteľnosť je možné zneužiť len v prípade použitia protokolu AMQP verzie 0-8, 0-9 a 0-91.

Dátum prvého zverejnenia varovania

19.06.2018

CVE

CVE-2018-8030

Zasiahnuté systémy

Apache Qpid Broker-J verzie 7.0.0 až 7.0.4

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. V prípade že aktualizáciu nie je možné vykonať, výrobca odporúča alternatívne postupy:
- **vypnutie limitu maximálnej veľkosti správ** nastavením kontextovej premennej "qpid.max_message_size" na hodnotu 0 alebo zápornú hodnotu. Zmenu nastavenia je možné vykonať priamo v konfiguračnom súbore brokera, prostredníctvom manažmentového rozhrania alebo použitím JVM "-Dqpid.max_message_size=0". Broker je následne potrebné reštartovať.
- **vypnutie podpory AMQP protokolov verzií 0-8, 0-9 a 0-91 na AMQP portoch**. Zmenu nastavenia je možné vykonať priamo v konfiguračnom súbore brokera alebo prostredníctvom manažmentového rozhrania. Príklad REST volania prostredníctvom curl:
curl --user <user-name> -X POST -d '{"protocols":["AMQP_1_0","AMQP_0_10"]}' \
https://<broker host>:<broker port>/api/latest/port/<port name>

Zdroje

https://issues.apache.org/jira/browse/QPID-8203
http://qpid.apache.org/releases/qpid-broker-j-7.0.5/release-notes.html
https://securitytracker.com/id/1041138

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SAJ Solar Inverter Information Disclosure Vulnerability

Popis

Výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti v produkte SAJ Solar Inverter.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému útočníkovi prostredníctvom webového rozhrania daného zariadenia (inverter_info.htm, english_main.htm) získať prístup k potenciálne citlivým údajom.

Dátum prvého zverejnenia varovania

25.06.2018

CVE

CVE-2018-12735

Zasiahnuté systémy

SAJ Solar Inverter

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a ich webovým rozhraniam zavedením zoznamu pre riadenie prístupov (ACL). Tiež odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2018-12735