BEZPEČNOSTNÝ BULLETIN

Týždeň 17. 04. 2019 - 23. 04. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Delta Industrial Automation CNCSoft ScreenEditor zraniteľnosti	Vysoká	**8.8**
02.	Zraniteľnosti v Drupal CMS	Vysoká	**8.8**
03.	GNU Wget zraniteľnosť	Vysoká	**8.8**
04.	UKcms zraniteľnosť	Vysoká	**8.8**
05.	Dovecot JSON Encoder zraniteľnosť	Vysoká	**7.5**
06.	Eclipse OpenJ9 Zraniteľnosť	Vysoká	**7.5**
07.	Python urlib3 zraniteľnosť	Vysoká	**7.5**
08.	GNU Tar Zraniteľnosť	Vysoká	**7.5**
09.	Zraniteľnosti Broadcom WiFi ovládačov	Vysoká	**7.1**
10.	Zraniteľnosť v produktoch Rockwell Automation MicroLogix 1400 and CompactLogix 5370	Vysoká	**7.1**
11.	Linux Kernel perf_event_open Zreniteľnosť	Stredná	**6.2**
12.	Apache Zeppelin viacero zraniteľností	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-114

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

Identifikátor

Delta Industrial Automation CNCSoft ScreenEditor zraniteľnosti

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na svoj produkt CNCSoft ScreenEditor, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.04.2019

CVE

CVE-2019-10947, CVE-2019-10949, CVE-2019-10951

Zasiahnuté systémy

Delta Industrial Automation CNCSoft ScreenEditor verzie staršie ako 1.00.89

Následky

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

Odporúčania

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

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-106-01

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

Identifikátor

Zraniteľnosti v Drupal CMS

Popis

Vývojári redakčného systému Drupal vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti nachádzajúce sa v komponentoch JQuery a Symfony umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

17.04.2019

CVE

CVE-2019-10909, CVE-2019-1091, CVE-2019-10910, CVE-2019-10911, CVE-2019-10912, CVE-2019-10913

Zasiahnuté systémy

Drupal verzie staršie ako 8.6.15., 8.5.15. a 7.66

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.
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.drupal.org/sa-core-2019-006
https://www.drupal.org/sa-core-2019-005
https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/
https://thehackernews.com/2019/04/drupal-security-update.html
https://symfony.com/blog/cve-2019-10909-escape-validation-messages-in-the-php-templating-engine
https://symfony.com/blog/cve-2019-10910-check-service-ids-are-valid
https://symfony.com/blog/cve-2019-10911-add-a-separator-in-the-remember-me-cookie-hash
https://symfony.com/blog/cve-2019-10912-prevent-destructors-with-side-effects-from-being-unserialized
https://symfony.com/blog/cve-2019-10913-reject-invalid-http-method-overrides

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

Identifikátor

GNU Wget zraniteľnosť

Popis

Vývojári linuxového nástroja GNU Wget vydali aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v implementačnej chybe v rámci irc.c a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvoreného súboru mohol zneužiť na vyvolanie pretečenia zásobníka a následné vykonanie škodlivého kódu alebo zneprístupnenie služby.

Dátum prvého zverejnenia varovania

23.04.2019

CVE

CVE-2019-5953

Zasiahnuté systémy

wget verzie staršie ako 1.20.2

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
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/viewAlert.x?alertId=60046

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

Identifikátor

UKcms zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti v redakčnom systéme UKcms.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov v rámci admin.php/admin/role/add.html. Uvedenú zraniteľnosť by vzdialený neautentifikovaný útočník mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku, vykonanie škodlivého kódu a získanie administrátorského prístupu do systému.

Dátum prvého zverejnenia varovania

22.04.2019

CVE

CVE-2019-10888

Zasiahnuté systémy

UKcms 1.1.10

Následky

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

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné bezpečnostné aktualizácie. V prípade, že sú Vaše webové stránky založené na redakčnom systéme MKCMS, odporúčame Vám 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://exchange.xforce.ibmcloud.com/vulnerabilities/159924

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

Identifikátor

Dovecot JSON Encoder zraniteľnosť

Popis

Vývojári e-mailového servera Dovecot vydali aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v komponente JSON Encoder.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní UTF-8 znakov a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených reťazcov v poliach hlavičky From alebo Subject mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

18.04.2019

CVE

CVE-2019-10691

Zasiahnuté systémy

Dovecot Dovecot verzie 2.3.0 až 2.3.5.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/159815
https://seclists.org/oss-sec/2019/q2/32

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

Identifikátor

Eclipse OpenJ9 Zraniteľnosť

Popis

Vývojári Eclipse Java Virtual Machine (JVM) OpenJ9 vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v komponente na overovanie JAVA bytekódu.
Bezpečnostná zraniteľnosť spočíva v implementačnej chybe a vzdialený neautentifikovaný útočník by ju mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

22.04.2019

CVE

CVE-2019-10245

Zasiahnuté systémy

IBM and Eclipse Foundation OpenJ9 verzie staršie ako 0.14

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/160010
https://bugs.eclipse.org/bugs/show_bug.cgi?id=545588

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

Identifikátor

Python urlib3 zraniteľnosť

Popis

Vývojári HTTP klienta pre Python urllib3 vydali aktualizáciu pre ich produkt, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nesprávnom spracovaní CA certifikátov a vzdialený neautentifikovaný útočník by ju mohol zneužiť na vytvorenie SSL spojení a získanie neoprávneného prístupu do systému.

Dátum prvého zverejnenia varovania

23.04.2019

CVE

CVE-2019-11324

Zasiahnuté systémy

Python urllib3 verzie staršej ako 1.24.2

Následky

Neoprávnený prístup do systému, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame 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.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=60048

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

Identifikátor

GNU Tar Zraniteľnosť

Popis

Vývojári linuxového nástroja GNU Tar vydali aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť vo funkcii pax_decode_header.
Bezpečnostná zraniteľnosť spočíva v implementačnej chybe v rámci zdrojového kódu sprase.c a vzdialený neautentifiovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených TAR súborov mohol zneužiť na zneprístupnenie služby.
Na uvedenú zraniteľnosť je v súčasnosti dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

22.04.2019

CVE

CVE-2019-9923

Zasiahnuté systémy

GNU Tar verzie staršie ako 1.32

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=60045

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.1
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosti Broadcom WiFi ovládačov

Popis

Bezpečnostní výskumníci objavili viacero zraniteľností v Broadcom Wifi ovládačoch wl a brcmfmac. Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

17.04.2019

CVE

CVE-2019-9500, CVE-2019-9501, CVE-2019-9502, CVE-2019-9503

Zasiahnuté systémy

Ovládač brcmfmac pre Broadcom FullMAC chipsety
Ovládač Broadcom wl pre Broadcom FullMAC a SoftMAC chipsety

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Používateľom odporúčame, aby sa pripájali iba na dôveryhodné WiFi siete.

Zdroje

https://www.kb.cert.org/vuls/id/166939/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.1
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť v produktoch Rockwell Automation MicroLogix 1400 and CompactLogix 5370

Popis

Spoločnosť Rockwell Automation vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť v riadiacich jednotkách MicroLogix 1400 a CompactLogix 5370.
Bližšie nešpecifikovanú bezpečnostnú zraniteľnosť by vzdialený neautentifikovaný útočník mohol zneužiť na podvrhnutie URL slúžiaceho na presmerovanie používateľov systému na stránky so škodlivým obsahom.

Dátum prvého zverejnenia varovania

23.04.2019

CVE

CVE-2019-10955

Zasiahnuté systémy

MicroLogix 1400 Controllers série A
MicroLogix 1400 Controllers série B verzie 15.002 a staršie
MicroLogix 1100 Controllers verize 14.00 a staršie
CompactLogix 5370 L1 controllers verzie 30.014 a staršie
CompactLogix 5370 L2 controllers verzie 30.014 a staršie
CompactLogix 5370 L3 controllers verzie 30.014 a staršie

Následky

Podvrhnutie škodlivého obsahu

Odporúčania

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

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-113-01
https://rockwellautomation.custhelp.com/app/answers/detail/a_id/1086288
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-10955

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Linux Kernel perf_event_open Zreniteľnosť

Popis

Vývojári Linux Kernel vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť vo funkcii perf_event_open.
Bezpečnostnú zraniteľnosť by lokálny neautentifikovaný útočník prostredníctvom zasielania špeciálne vytvorených požiadaviek mohol zneužiť na neoprávnený prístup k citlivým údajom z setuid programov.

Dátum prvého zverejnenia varovania

22.04.2019

CVE

CVE-2019-3901

Zasiahnuté systémy

Linux Kernel 4.7.0

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=79c9ce57eb2d5f1497546a3946b4ae21b6fdc438
https://exchange.xforce.ibmcloud.com/vulnerabilities/159973

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

Identifikátor

Apache Zeppelin viacero zraniteľností

Popis

Spoločnosť Apache vydala aktualizáciu na svôj produkt Zeppelin ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nesprávnym spracovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať Cross-Site Scripting (XSS) útok pomocou ktorého môže získať neoprávnený prístup k citlivým dátam.

Dátum prvého zverejnenia varovania

23.04.2019

CVE

CVE-2017-12619, CVE-2018-1317, CVE-2018-1328

Zasiahnuté systémy

Apache Zeppelin verzie staršie ako 0.8.0

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame 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.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/160019
https://exchange.xforce.ibmcloud.com/vulnerabilities/160020
https://exchange.xforce.ibmcloud.com/vulnerabilities/160021