BEZPEČNOSTNÝ BULLETIN

Týždeň 11. 04. 2018 – 17. 04. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Multiple Vulnerabilities in Moxa EDR-810 Industrial Secure Router	Vysoká	**8.8**
02.	Multiple Vulnerabilities in Adobe Products	Vysoká	**8.8**
03.	idreamsoft iCMS Vulnerability	Vysoká	**8.8**
04.	Hewlett Packard Enterprise Universal CMDB	Vysoká	**8.4**
05.	Perl Multiple Vulnerabilities	Vysoká	**7.8**
06.	F5 BIG-IP Multiple Vulnerabilities	Vysoká	**7.5**
07.	Apache Solr XXE Vulnerability	Vysoká	**7.5**
08.	VMware vRealize Automation (vRA) Multiple Vulnerabilities	Stredná	**6.1**
09.	IBM WebSphere Portal XSS Vulnerability	Stredná	**5.4**

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-036

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

Identifikátor

Multiple Vulnerabilities in Moxa EDR-810 Industrial Secure Router

Popis

Spoločnosť Moxa vydala bezpečnostné aktualizácie na priemyselné smerovače Moxa EDR-810, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšie zraniteľnosti sa nachádzajú v skriptoch */goform/net_Web_get_value, /goform/WebRSAKEYGen, /goform/net_WebPingGetValue, /goform/net_Web_get_value, /goform/net_WebCSRGen* a vzdialený autentifikovaný útočník by ich mohol zneužiť na eskaláciu privilégií a vykonanie príkazov s oprávneniami úrovne root.

Ostatné zraniteľnosti by vzdialený autentifikovaný útočník mohol zneužiť na zneprístupnenie služby a neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

13.04.2018

CVE

CVE-2017-12120, CVE-2017-12121, CVE-2017-12123, CVE-2017-12124, CVE-2017-12125, CVE-2017-12126, CVE-2017-12127, CVE-2017-12128, CVE-2017-12129, CVE-2017-14432, CVE-2017-14433, CVE-2017-14432, CVE-2017-14435, CVE-2017-14436, CVE-2017-14437, CVE-2017-14438, CVE-2017-14439

Zasiahnuté systémy

Moxa EDR-810 firmware V4.1 build 17030317

Následky

Eskalácia privilégií, Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých zariadení.

Zdroje

https://blog.talosintelligence.com/2018/04/vuln-moxa-edr-810.html

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

Identifikátor

Multiple Vulnerabilities in Adobe Products

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie, ktoré riešia viacero bezpečnostných zraniteľností v produktoch PhoneGape Push, Digital Editions, InDesign CC, Experience Manager, ColdFusion a Flash Player.
Najzávažnejšie zraniteľnosti sa nachádzajú v produktoch Adobe Flash Player a InDesign a vzdialený neautentifikovaný útočník by ich mohol zneužiť na vykonanie škodlivého kódu v kontexte prihláseného používateľa. Zraniteľnosti v Adobe Experience Manager a ColdFusion by vzdialený neautentifikovaný útočník mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku a získanie prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

10.04.2018

CVE

CVE-2018-4925, CVE-2018-4926, CVE-2018-4927, CVE-2018-4928, CVE-2018-4929, CVE-2018-4930, CVE-2018-4931, CVE-2018-4932, CVE-2018-4933, CVE-2018-4934, CVE-2018-4935, CVE-2018-4936, CVE-2018-4937, CVE-2018-4938, CVE-2018-4939, CVE-2018-4940, CVE-2018-4941, CVE-2018-4942, CVE-2018-4943

Zasiahnuté systémy

Adobe PhoneGap Push plugin verzie staršie ako 1.8.0, Adobe Digital Editions verzie staršie ako 4.5.7, Adobe InDesign CC verzie staršie ako 13.0, Adobe Experience Manager verzie 6.0 až 6.3, Adobe Flash Player verzie staršie ako 29.0.0.113, Adobe ColdFusion Update 5 a staršie verzie, Adobe ColdFusion 11 Update 13 a staršie verzie

Následky

Vykonanie škodlivého kódu, Eskalácia privilégií, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://helpx.adobe.com/security/products/phonegap/apsb18-15.html
https://helpx.adobe.com/security/products/Digital-Editions/apsb18-13.html
https://helpx.adobe.com/security/products/indesign/apsb18-11.html
https://helpx.adobe.com/security/products/experience-manager/apsb18-10.html
https://helpx.adobe.com/security/products/flash-player/apsb18-08.html
https://helpx.adobe.com/security/products/coldfusion/apsb18-14.html

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

Identifikátor

idreamsoft iCMS Vulnerability

Popis

Systém pre správu obsahu iCMS od spoločnosti idreamsoft obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený útočník mohol zneužiť na realizáciu CSRF (Cross-Site Request Forgery) útoku.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov v rámci *admincp.php* a útočníkovi umožňuje prostredníctvom podvrhnutia špecifickej HTTP požiadavky vytvoriť administrátorský účet.

Dátum prvého zverejnenia varovania

15.04.2018 (posledná aktualizácia 17.04.2018)

CVE

CVE-2018-10117

Zasiahnuté systémy

idreamsoft iCMS 7.0.7

Následky

Neoprávnený prístup do systému, Neoprávnená zmena v systéme

Odporúčania

Odporúčame uistiť sa, či Vaše webové aplikácie nie sú založené na systéme pre správu obsahu iCMS v zraniteľných verziách. V prípade, že áno, nakoľko v súčasnosti nie sú dostupné aktualizácie, odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://github.com/idreamsoft/iCMS/issues/20
https://exchange.xforce.ibmcloud.com/vulnerabilities/141645

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

Identifikátor

Hewlett Packard Enterprise Universal CMDB

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v produkte Universal CMDB.
Uvedenú zraniteľnosť by lokálny neautentifikovaný útočník mohol zneužiť na eskaláciu privilégií a vykonanie škodlivého kódu v kontexte SYSTEM.

Dátum prvého zverejnenia varovania

12.04.2018

CVE

CVE-2018-6491

Zasiahnuté systémy

HP UCMDB Configuration Manager Software verzie 10.20, 10.21, 10.22, 10.30, 10.31, 10.32, 10.33, 11.0

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03141180
https://exchange.xforce.ibmcloud.com/vulnerabilities/141555
https://www.zerodayinitiative.com/advisories/ZDI-18-299/

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

Identifikátor

Perl Multiple Vulnerabilities

Popis

Perl.org vydala bezpečnostnú aktualizáciu na Perl, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť spočíva v nesprávnom vyhodnocovaní regulárnych výrazov v rámci funkcie *S_regatom()* v *regcomp.c* a lokálny útočník by ju mohol zneužiť na vykonanie škodlivého kódu.
Ďalšie zraniteľnosti by lokálny útočník mohol zneužiť na zneprístupnenie služby alebo neoprávnený prístup k citlivými údajom.

Dátum prvého zverejnenia varovania

15.04.0218

CVE

CVE-2018-6797, CVE-2018-6798, CVE-2018-6913

Zasiahnuté systémy

Perl verzie pred 5.26.2

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://search.cpan.org/~shay/perl/pod/perldelta.pod
https://www.securitytracker.com/id/1040681

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

Identifikátor

F5 BIG-IP Multiple Vulnerabilities

Popis

Spoločnosť F5 vydala bezpečnostné aktualizácie na svoje produkty BIG-IP, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť spočíva v nesprávnom spracovaní paketov v komponente TMM (Traffic Management Microkernel) a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálnej sekvencie paketov mohol zneužiť na zneprístupnenie služby. Zraniteľnosť je možné zneužiť len na IPv6 virtuálnych serveroch.
Zraniteľnosti v Apache moduloch *apache_auth_token_mod* a *mod_auth_f5_auth_token* by vzdialený autentifikovaný útočník mohol zneužiť na získanie klientskych SSL certifikátov používaných na vzájomnú autentifikáciu medzi Enterprise Manager a BIG-IP zariadeniami.

Dátum prvého zverejnenia varovania

12.04.2018 (posledná aktualizácia 16.04.2018)

CVE

CVE-2018-5506, CVE-2018-5507, CVE-2018-5508, CVE-2018-5510, CVE-2018-5511

Zasiahnuté systémy

F5 BIG-IP (Analytics, LTM, AAM, AFM, APM, ASM, DNS, Edge, Gateway, GTM Link Controller, PEM, WebAccelerator, WebSafe) 11.2.1, 11.5.1 - 11.5.5, 11.6.0 - 11.6.2, 12.1.0 - 12.1.3.1, 13.0.0
F5 Enterprise Manager 3.1.1

Následky

Zneprístupnenie služby, Eskalácia privilégií

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://support.f5.com/csp/article/K77671456
https://support.f5.com/csp/article/K65355492
https://support.f5.com/csp/article/K52521791
https://support.f5.com/csp/article/K10329515
https://support.f5.com/csp/article/K30500703

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

Identifikátor

Apache Solr XXE Vulnerability

Popis

Produkt Apache Solr obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na realizáciu XXE (XML External Entity Expansion) útoku.
Zraniteľnosť sa nachádza v module DataImportHandler a útočník by ju mohol prostredníctvom podvrhnutia špeciálneho súboru zneužiť na získanie prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

11.04.2018

CVE

CVE-2018-1308

Zasiahnuté systémy

Apache Solr verzie 1.2 až 6.6.2
Apache Solr verzie 7.0.0 až 7.2.1

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://issues.apache.org/jira/browse/SOLR-11971
https://tools.cisco.com/security/center/viewAlert.x?alertId=57447

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

Identifikátor

VMware vRealize Automation (vRA) Multiple Vulnerabilities

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie, ktoré riešia viacero zraniteľností v produkte vRealize Automation.
Najzávažnejšia zraniteľnosť spočíva v nesprávnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ju mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku a v prípade jeho úspešnosti vykonať škodlivý skript a získať prihlasovacie údaje.

Dátum prvého zverejnenia varovania

12.04.2018

CVE

CVE-2018-6958, CVE-2018-6959

Zasiahnuté systémy

VMware vRealize Automation verzie 7.0 až 7.3

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2018-0009.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/141625
https://exchange.xforce.ibmcloud.com/vulnerabilities/141626

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.4**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

IBM WebSphere Portal XSS Vulnerability

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt IBM WebSphere Portal, ktorá opravuje bezpečnostnú zraniteľnosť vo webovom používateľskom rozhraní.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený autentifikovaný útočník by ju mohol zneužiť na realizáciu XSS (Cross Site Scripting) útoku a v prípade jeho úspešnosti vykonať škodlivý JavaScript kód a získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

10.04.2018 (posledná aktualizácia 11.04.2018)

CVE

CVE-2018-1445

Zasiahnuté systémy

IBM WebSphere Portal verzie 8.0 Cumulative Fix 22
IBM WebSphere Portal verzie 8.5 Cumulative Fix 15
IBM WebSphere Portal verzie 9.0 Cumulative Fix 15

Následky

Vykonanie škodlivého kódu, Neprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

http://www-01.ibm.com/support/docview.wss?uid=swg22015407
https://www.securitytracker.com/id/1040647