BEZPEČNOSTNÝ BULLETIN

Týždeň 21. 02. 2018 – 27. 02. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Micro Focus UCMDB Vulnerability	Vysoká	**8.1**
02.	Drupal core Multiple Vulnerabilities	Vysoká	**7.6**
03.	Digium Asterisk Multiple Denial of Service Vulnerabilities	Vysoká	**7.5**
04.	Squid ESI Response Processing Denial of Service Vulnerability	Vysoká	**7.4**
05.	Apple iOS and macOS High Sierra CoreText Heap Corruption Vulnerability	Stredná	**6.5**
06.	ImageMagick Denial of Service Vulnerabilities	Stredná	**6.5**
07.	ADMS netCADOPS Bounds Checking Vulnerability	Stredná	**5.8**
08.	phpMyAdmin Cross Site Scripting Vulnerability	Stredná	**5.4**
09.	IBM Rational Rhapsody Design Manager Cross-Site Scripting Vulnerability	Stredná	**5.4**
10.	Apache Tomcat Security Vulnerabilities	Stredná	**4.8**

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2858*

SK-CERT
Naša značka:
02049/2018/TS/OKB-011

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

Identifikátor

Micro Focus UCMDB Vulnerability

Popis

Spoločnosť Micro Focus vydala bezpečnostnú aktualizáciu na svoj produkt Universal Configuration Manager, ktorá opravuje bezpečnostnú zraniteľnosť. Výrobcom bližšie nešpecifikovanú bezpečnostnú zraniteľnosť by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

21.02.2018

CVE

CVE-2018-6488

Zasiahnuté systémy

Micro Focus Universal Configuration Manager Software verzie 4.10, 4.11, 4.12

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03086019
https://nvd.nist.gov/vuln/detail/CVE-2018-6488

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.6**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Drupal Core Multiple Vulnerabilities

Popis

Vývojový tím redakčného systému Drupal vydal aktualizáciu svojho produktu, ktorá rieši viacero bezpečnostných zraniteľností spôsobených nedostatočným overovaním používateľských vstupov a nedostatkami v implementácii mechanizmov zabezpečenia. Bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne vytvorených súborov zneužiť na neoprávnený prístup k citlivým údajom a tiež neoprávnený prístup do zasiahnutého systému.

Dátum prvého zverejnenia varovania

21.02.2018

CVE

CVE-2017-6926, CVE-2017-6927, CVE-2017-6928, CVE-2017-6929, CVE-2017-6930, CVE-2017-6931, CVE-2017-6932

Zasiahnuté systémy

Drupal 7 verzie staršie ako 7.57
Drupal 8 verzie staršie ako 8.4.5

Následky

Neoprávnený prístup k citlivým údajom, Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.drupal.org/sa-core-2018-001
https://www.securityweek.com/several-vulnerabilities-patched-drupal
https://www.securitytracker.com/id/1040430

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

Identifikátor

Digium Asterisk Multiple Denial of Service Vulnerabilities

Popis

Spoločnosť Digium vydala bezpečnostnú aktualizáciu na produkt Asterisk, ktorý opravuje viacero bezpečnostných zraniteľností, ktoré by vzdialený útočník mohol zneužiť na zneprístupnenie služieb.
Najzávažnejšie zraniteľnosti spočívajú v nesprávnom spracovaní SUBSCRIBE požiadaviek a nesprávnom vyhodnocovaní identifikátorov payloadov.
Ďalšie zraniteľnosti spočívajú v nesprávnom spracovaní INVITE správ doručených prostredníctvom TCP alebo TLS spojení a nedostatočnou implementáciou mechanizmov overovania dĺžky WebSocket rámcov.

Dátum prvého zverejnenia varovania

22.02.2018

CVE

CVE-2018-7284, CVE-2018-7285, CVE-2018-7286, CVE-2018-7287

Zasiahnuté systémy

Digium Asterisk verzie 15 (.0, .1.0, .1.1, .1.2, .1.3, .1.4)
Digium Asterisk verzie 14 (.0 - .7.0,.7.1,.7.2,.7.3,.7.4)
Digium Asterisk verzie 13 (.0 - .18.0, .18.1, .18.2, .18.3, .18.4)

Následky

Zneprístupnenie služieb

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

http://downloads.asterisk.org/pub/security/AST-2018-001.html
http://downloads.asterisk.org/pub/security/AST-2018-004.html
http://downloads.asterisk.org/pub/security/AST-2018-005.html
http://downloads.asterisk.org/pub/security/AST-2018-006.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.4**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Squid ESI Response Processing Denial of Service Vulnerability

Popis

Vývojári webového proxy Squid vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostné zraniteľnosti v procese spracovania ESI (Edge Side Includes) odpovedí a HTTP požiadaviek.
Bezpečnostná zraniteľnosť spočíva v nesprávnom spracovaní ESI a HTTP požiadaviek a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne upravených ESI/HTTP požiadaviek mohol zneužiť na zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

19.01.2018 (aktualizácia 23.01.2018)

CVE

CVE-2018-1000024, CVE-2018-1000027

Zasiahnuté systémy

Squid 3.x až 3.5.27
Squid 4.x až 4.0.22

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

http://www.squid-cache.org/Advisories/SQUID-2018_1.txt
http://www.squid-cache.org/Advisories/SQUID-2018_2.txt
https://tools.cisco.com/security/center/viewAlert.x?alertId=56920

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

Identifikátor

Apple iOS and macOS High Sierra CoreText Heap Corruption Vulnerability

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje produkty iOS, macOS High Sierra, tvOS a watchOS, ktoré opravujú bezpečnostnú zraniteľnosť spočívajúcu v nesprávnom zaobchádzaní s objektami uloženými v pamäti.
Bezpečnostnú zraniteľnosť by vzdialený útočník mohol prostredníctvom podvrhnutia špecifického textového reťazca alebo súboru zneužiť na zneprístupnenie služieb a potenciálne vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

19.02.2018

CVE

CVE-2018-4124

Zasiahnuté systémy

iOS 11.2.5 a staršie
macOS High Sierra 10.13.3 a staršie
tvOS 11.2.6 a staršie
watchOS 4.2.3 a staršie

Následky

Zneprístupnenie služby, Potenciálne vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://support.apple.com/en-us/HT208535
https://support.apple.com/en-us/HT208534
https://packetstormsecurity.com/files/146484/Apple-Security-Advisory-2018-02-19-4.html
https://packetstormsecurity.com/files/146483/Apple-Security-Advisory-2018-02-19-3.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=56869

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

Identifikátor

ImageMagick Denial of Service Multiple Vulnerabilities

Popis

Vývojári grafického editora ImageMagick vydali aktualizáciu svojho produktu, ktorá rieši bezpečnostné zraniteľnosti spôsobené nesprávnym overovaním dát v rámci funkcií v *coders/tiff.c* a *coders/webp.c*.
Bezpečnostné zraniteľnosti by vzdialený útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vyvolanie pretečenia zásobníka a následné zneprístupnenie služieb zasiahnutého systému.

Dátum prvého zverejnenia varovania

23.02.2018

CVE

CVE-2018-7443, CVE-2018-7470

Zasiahnuté systémy

ImageMagick 7.0.7 (-22)

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://github.com/ImageMagick/ImageMagick/issues/998
https://github.com/ImageMagick/ImageMagick/issues/999
https://tools.cisco.com/security/center/viewAlert.x?alertId=56931

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.8**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

ADMS netCADOPS Bounds Checking Vulnerability

Popis

Spoločnosť ABB vydala bezpečnostné aktualizácie na svoj produkt netCADOPS Web Application, ktoré opravujú bezpečnostnú zraniteľnosť vo webovom rozhraní.
Bezpečnostná zraniteľnosť je spôsobená nesprávnym nastavením autentifikačného rozhrania a lokálny útočník by ju mohol zneužiť na neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

16.02.2018

CVE

CVE-2018-5477

Zasiahnuté systémy

netCADOPS Web Application verzie 3.4 a staršie
netCADOPS Web Application verzie 7.1 a staršie
netCADOPS Web Application verzie 7.2x a staršie
netCADOPS Web Application verzie 8.0 a staršie
netCADOPS Web Application verzie 8.1 a staršie

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

http://search.abb.com/library/Download.aspx?DocumentID=9AKK107045A9592&LanguageCode=en&DocumentPartId=&Action=Launch
https://ics-cert.us-cert.gov/advisories/ICSA-18-051-01

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

Identifikátor

phpMyAdmin Cross Site Scripting Vulnerability

Popis

Produkt phpMyAdmin obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený autentifikovaný útočník mohol zneužiť na realizáciu XSS (Cross Site Scripting) útoku a v prípade jeho úspešnosti vykonať škodlivý kód. Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov vo funkcii *db_central_columns.php*.

Dátum prvého zverejnenia varovania

20.02.2018 (posledná aktualizácia 21.22.2018)

CVE

CVE-2018-7260

Zasiahnuté systémy

phpMyAdmin verzie 4.4.7, 4.7, 4.7.1, 4.7.2, 4.7.3, 4.7.4, 4.7.5, 4.7.6, 4.7.7

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://www.phpmyadmin.net/security/PMASA-2018-1/
https://tools.cisco.com/security/center/viewAlert.x?alertId=56914
https://nvd.nist.gov/vuln/detail/CVE-2018-7260

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

Identifikátor

IBM Rational Rhapsody Design Manager Cross-Site Scripting Vulnerability

Popis

Webové rozhranie produktu IBM Rational Rhapsody Design Manager obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený autentifikovaný útočník mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku a v prípade jeho úspešnosti vykonať škodlivý JavaScript kód. Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov.

Dátum prvého zverejnenia varovania

21.02.2018 (posledná aktualizácia 22.02.2018)

CVE

CVE-2017-1462

Zasiahnuté systémy

IBM Rational Rhapsody Design Manager 5.0.0, 5.0.1, 5.0.2
IBM Rational Rhapsody Design Manager 6.0.0, 6.0.1, 6.0.2, 6.0.3, 6.0.4

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

http://www.ibm.com/support/docview.wss?uid=swg22013739
https://tools.cisco.com/security/center/viewAlert.x?alertId=56870

BEZPEČNOSTNÝ BULLETIN

Týždeň 21. 02. 2018 – 27. 02. 2018

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 4.8**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache Tomcat Security Vulnerabilities

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt Apache Tomcat, ktorá opravuje bezpečnostné zraniteľnosti v komponente Servlets.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii mechanizmov zabezpečenia a vzdialený útočník by ich prostredníctvom podvrhnutia upravenej adresy URL mohol zneužiť na neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

23.02.2018

CVE

CVE-2018-1304, CVE-2018-1305

Zasiahnuté systémy

Apache Tomcat 9.0.0.M1 až 9.0.4
Apache Tomcat 8.5.0 až 8.5.27
Apache Tomcat 8.0.0.RC1 až 8.0.49
Apache Tomcat 7.0.0 až 7.0.84

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://lists.apache.org/thread.html/d3354bb0a4eda4acc0a66f3eb24a213fdb75d12c7d16060b23e65781@%3Cannounce.tomcat.apache.org%3E
http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.5
https://www.securitytracker.com/id/1040428

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2858*

SK-CERT
Naša značka:
02049/2018/TS/OKB-011