BEZPEČNOSTNÝ BULLETIN

Týždeň 02. 01. 2019 - 08. 01. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Adobe Acrobat and Reader zraniteľnosti	Vysoká	**8.8**
02.	Apache Oozie zraniteľnosť	Vysoká	**8.7**
03.	Artifex Software Ghostscript Zraniteľnosť	Vysoká	**7.8**
04.	Dell RSA Authentication Manager zraniteľnosť	Vysoká	**7.7**
05.	Hetronic Nova-M zraniteľnosť	Vysoká	**7.6**
06.	Kibana zraniteľnosti	Vysoká	**7.5**
07.	Apache Thrift zraniteľnosti	Vysoká	**7.5**
08.	Yokogawa Vnet/IP Open Communication Driver Denial of Service (DoS) zraniteľnosť	Vysoká	**7.5**
09.	Clean My Mac X zraniteľnosti	Vysoká	**7.1**
10.	Apache NiFi viacero zraniteľností	Vysoká	**7.1**
11.	Apache Tika zraniteľnosť	Stredná	**6.5**

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-005

BEZPEČNOSTNÝ BULLETIN

Týždeň 02. 01. 2019 - 08. 01. 2019

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

Identifikátor

Adobe Acrobat and Reader zraniteľnosti

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty Adobe Acrobat a Reader, ktoré opravujú dve bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti umožňujú vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.01.2019

CVE

CVE-2018-16011, CVE-2018-16018

Zasiahnuté systémy

Adobe Acrobat DC verzie staršie ako 2019.010.20069; 2017.011.30113; 2015.006.30464
Adobe Acrobat Reader DC verzie staršie ako 2019.010.20069; 2017.011.30113; 2015.006.30464

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://helpx.adobe.com/security/products/acrobat/apsb19-02.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-adobe-acrobat-and-reader-could-allow-for-arbitrary-code-execution-apsb19-02_2019-001/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.7
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache Oozie zraniteľnosť

Popis

Vývojári systému Apache Oozie vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému autentifikovanému útočníkovi získať prístupové práva ostatných používateľov.

Dátum prvého zverejnenia varovania

19.12.2018

CVE

CVE-2018-11799

Zasiahnuté systémy

Apache Oozie verzie staršie ako 5.1.0

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://lists.apache.org/thread.html/347e7a8cb86014b7ca37e49eb00b8d088203bdc0bcfb4799f8e5955a@%3Cuser.oozie.apache.org%3E
https://tools.cisco.com/security/center/viewAlert.x?alertId=59384

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

Identifikátor

Artifex Software Ghostscript Zraniteľnosť

Popis

Spoločnosť Artifex Software vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť v produkte Artifex Software Ghostscript.
Bezpečnostná zraniteľnosť spočíva v nesprávnom overovaní dátových typov v operátore setpattern a lokálny neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených PostScript súborov mohol zneužiť na vykonanie škodlivého kódu alebo zneprístupnenie služby.

Dátum prvého zverejnenia varovania

07.01.2019

CVE

CVE-2018-19134

Zasiahnuté systémy

Artifex Software Ghostscript verzie staršie ako 9.26

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://git.ghostscript.com/?p=ghostpdl.git&a=commit&h=693baf02152119af6e6afd30bb8ec76d14f84bbf
https://tools.cisco.com/security/center/viewAlert.x?alertId=59387

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.7
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Dell RSA Authentication Manager zraniteľnosť

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoj produkt RSA Authentication Manager, ktorá opravuje bezpečnostnú zraniteľnosť v Quick Setup komponente.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravenej licencie získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

03.01.2019

CVE

CVE-2018-15782

Zasiahnuté systémy

RSA Authentication Manager verzie staršie ako 8.4

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://seclists.org/fulldisclosure/2019/Jan/18
https://exchange.xforce.ibmcloud.com/vulnerabilities/155153

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

Identifikátor

Hetronic Nova-M zraniteľnosť

Popis

Spoločnosť Hetronic vydala bezpečnostnú aktualizáciu na svoje produkty Nova-M, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje autentifikovanému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente, prostredníctvom odchytávania a replikácie sieťovej prevádzky spôsobiť neoprávnené zmeny v systéme a zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

03.01.2019

CVE

CVE-2018-19023

Zasiahnuté systémy

Nova-M verzie staršie ako r161
ES-CAN-HL verzie staršie ako Main r1864, Estop_v24
BMS-HL verzie staršie ako Main r1175, Estop_v24
MLC verzie staršie ako Main r1600, Estop_v24
DC Mobile verzie staršie ako Main r515, Estop_v24

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

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

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-003-03

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

Identifikátor

Kibana zraniteľnosti

Popis

Vývojári vyhľadávacieho nástroja Kibana vydali aktualizáciu svojho produktu, ktorá rieši viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov pri generovaní PDF správ a umožňuje vzdialenému neautentifikovanému útočníkovi získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

07.01.2019

CVE

CVE-2018-17245, CVE-2018-17246

Zasiahnuté systémy

Kibana verzie staršie ako 6.4.3 a 5.6.13

Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://discuss.elastic.co/t/elastic-stack-6-4-3-and-5-6-13-security-update/155594
https://tools.cisco.com/security/center/viewAlert.x?alertId=59386
https://tools.cisco.com/security/center/viewAlert.x?alertId=59385

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 nástroja Apache Thrift vydali aktualizáciu svojho produktu, ktorá rieši viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní prístupov v Node.js komponente a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených požiadaviek získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

07.01.2019

CVE

CVE-2018-11798, CVE-2018-1320

Zasiahnuté systémy

Apache Thrift 0.12.0

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/155198
https://exchange.xforce.ibmcloud.com/vulnerabilities/155199

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

Identifikátor

Yokogawa Vnet/IP Open Communication Driver Denial of Service (DoS) zraniteľnosť

Popis

Spoločnosť Yokogawa vydala bezpečnostné aktualizácie na viaceré svoje produkty, ktoré opravujú bezpečnostnú zraniteľnosť v Vnet/IP Open Communication Driver.
Bezpečnostná zraniteľnosť umožňuje vzdialenému neautentifikovanému útočníkovi spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

21.12.2018

CVE

CVE-2018-16196

Zasiahnuté systémy

CENTUM CS 3000 (R3.05.00 - R3.09.50),
CENTUM CS 3000 Entry Class (R3.05.00 - R3.09.50),
CENTUM VP (R4.01.00 - R6.03.10),
CENTUM VP Entry Class (R4.01.00 - R6.03.10),
Exaopc (R3.10.00 - R3.75.00),
PRM (R2.06.00 - R3.31.00),
ProSafe-RS (R1.02.00 - R4.02.00),
FAST/TOOLS (R9.02.00 - R10.02.00), and
B/M9000 VP (R6.03.01 - R8.01.90).

Následky

Zneprístupnenie služby

Odporúčania

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

Zdroje

https://web-material3.yokogawa.com/YSAR-18-0008-E.pdf
https://ics-cert.us-cert.gov/advisories/ICSA-19-003-02

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

Identifikátor

Clean My Mac X zraniteľnosti

Popis

Spoločnosť MacPaw vydala bezpečnostné aktualizácie na svoj produkt Clean My Mac, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú lokálnemu neautentifikovanému útočníkovi eskalovať svoje privilégiá na zraniteľnom systéme.

Dátum prvého zverejnenia varovania

02.01.2019

CVE

CVE-2018-4047, CVE-2018-4046, CVE-2018-4045, CVE-2018-4044, CVE-2018-4043, CVE-2018-4042, CVE-2018-4041, CVE-2018-4037, CVE-2018-4036, CVE-2018-4035, CVE-2018-4034, CVE-2018-4033, CVE-2018-4032

Zasiahnuté systémy

Clean My Mac X verzie staršie ako 4.1.0

Následky

Eskalácia privilégií
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0706
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0715
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0707

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

Identifikátor

Apache NiFi viacero zraniteľností

Popis

Vývojári softvéru Apache NiFi vydali aktualizáciu svojho produktu, ktorá rieši viacero chýb a bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nesprávnym spracovaním citlivých údajov v API koncovom bode pre nahrávanie šablón a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom cross-site request forgery útoku vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

26.10.2018

CVE

CVE-2018-17195

Zasiahnuté systémy

Apache NiFi verzie staršie ako 1.8.0

Následky

Vykonanie škodlivého kódu
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://nifi.apache.org/security.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=59380
https://tools.cisco.com/security/center/viewAlert.x?alertId=59379
https://tools.cisco.com/security/center/viewAlert.x?alertId=59381
https://tools.cisco.com/security/center/viewAlert.x?alertId=59377

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

Identifikátor

Apache Tika zraniteľnosť

Popis

Vývojári nástroja pre spracovanie metadát Apache Tika vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť vo funkcii SQLite3Parser.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov zasiahnutým systémom a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného SQLite súboru spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

07.01.2019

CVE

CVE-2018-17197

Zasiahnuté systémy

Apache Tika verzie staršie ako 1.20

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59392
https://lists.apache.org/thread.html/7c021a4ea2037e52e74628e17e8e0e2acab1f447160edc8be0eae6d3@%3Cdev.tika.apache.org%3E