BEZPEČNOSTNÝ BULLETIN

Týždeň 29. 05. 2019 - 04. 06. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Apache Hadoop zraniteľnosť	Vysoká	**8.8**
02.	Jenkins plugins viacero zraniteľností	Vysoká	**8.8**
03.	Apple AirPort Base Station Firmware zraniteľnosti	Vysoká	**8.8**
04.	Apple iCloud a iTunes zraniteľnosti	Vysoká	**8.8**
05.	Apache Camel zraniteľnosť	Vysoká	**7.5**
06.	Nmap zraniteľnosť	Vysoká	**7.5**
07.	Emerson Ovation OCR400 Controller zraniteľnosti	Stredná	**6.8**
08.	AVEVA Vijeo Citect a CitectSCADA zraniteľnosť	Stredná	**6.5**
09.	Supra Smart Cloud TV zraniteľnosť	Stredná	**6.3**

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:
01380/2019/TS/OKB-152

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

Identifikátor

Apache Hadoop zraniteľnosť

Popis

Vývojári z Apache Software Foundation vydali bezpečnostnú aktualizáciu na svoj produkt Hadoop, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

30.05.2019

CVE

CVE-2018-8029

Zasiahnuté systémy

Apache Hadoop verzie staršie ako 3.1.1, 2.9.2 a 2.8.5

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://seclists.org/oss-sec/2019/q2/132
https://exchange.xforce.ibmcloud.com/vulnerabilities/161812
https://hadoop.apache.org/cve_list.html

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

Identifikátor

Jenkins plugins viacero zraniteľností

Popis

Vývojári produktu Jenkins vydali bezpečnostné aktualizácie na zásuvné moduly, ktoré opravujú viacero bezpečnostných zraniteľností. Najvážnejšia bezpečnostná zraniteľnosť v Jenkins Pipeline Remote Loader Plugin je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom špeciálne vytvorenej požiadavky získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

31.05.2019

CVE

CVE-2019-10321, CVE-2019-10322, CVE-2019-10323, CVE-2019-10324, CVE-2019-10325, CVE-2019-10326, CVE-2019-10327, CVE-2019-10328, CVE-2019-10329, CVE-2019-10330

Zasiahnuté systémy

Artifactory Plugin verzie staršie ako 3.2.2 (vrátane)
Gitea Plugin verzie staršie ako 1.1.2
InfluxDB Plugin verzie staršie ako 1.22
Pipeline Maven Loader Plugin verzie staršie ako 3.7.1
Pipeline Remote Loader Plugin 1.5
Warnings Next Generation Plugin verzie staršie ako 5.1.0

Následky

Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.
V prípade Artifactory Pluginu administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://jenkins.io/security/advisory/2019-05-31/
https://nvd.nist.gov/vuln/detail/CVE-2019-10328

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

Identifikátor

Apple AirPort Base Station Firmware zraniteľnosti

Popis

Spoločnosť Apple zverejnila informácie o bezpečnostných zraniteľnostiach vo svojom produkte AirPort Base Station Firmware. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.05.2019

CVE

CVE-2018-6918, CVE-2019-7291, CVE-2019-8572, CVE-2019-8575, CVE-2019-8578, CVE-2019-8580, CVE-2019-8581, CVE-2019-8588

Zasiahnuté systémy

Apple AirPort Base Station Firmware verzie staršie ako 7.9.1

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.apple.com/en-us/HT210090

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

Identifikátor

Apple iCloud a iTunes zraniteľnosti

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje produkty iTunes for Windows a iCloud for Windows, ktoré opravujú viacero bezpečnostných zraniteľností v komponentoch SQLite a WebKit. Najvážnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.05.2019

CVE

CVE-2019-6237, CVE-2019-8571, CVE-2019-8577, CVE-2019-8583, CVE-2019-8584, CVE-2019-8586, CVE-2019-8587, CVE-2019-8594, CVE-2019-8595, CVE-2019-8596, CVE-2019-8597, CVE-2019-8598, CVE-2019-8600, CVE-2019-8601, CVE-2019-8602, CVE-2019-8607, CVE-2019-8608, CVE-2019-8609, CVE-2019-8610, CVE-2019-8611, CVE-2019-8615, CVE-2019-8619, CVE-2019-8622, CVE-2019-8623, CVE-2019-8628

Zasiahnuté systémy

iCloud for Windows staršie ako 7.12
iTunes for Windows staršie ako 12.9.5

Následky

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

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://support.apple.com/en-us/HT210125
https://support.apple.com/en-us/HT210124

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

Identifikátor

Apache Camel zraniteľnosť

Popis

Vývojári z Apache Software Foundation vydali bezpečnostnú aktualizáciu na svoj produkt Camel, ktorá opravuje bezpečnostnú zraniteľnosť v komponente camel-xmljson.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom XXE útoku získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

24.05.2019

CVE

CVE-2019-0188

Zasiahnuté systémy

Apache Tomcat verzie staršie ako 2.24.0

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://lists.apache.org/thread.html/00118387610522b107cbdcec5369ddd512b576ff0236a02bfca12f44@%3Cusers.camel.apache.org%3E
https://tools.cisco.com/security/center/viewAlert.x?alertId=60238

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

Identifikátor

Nmap zraniteľnosť

Popis

Vývojári Nmap zverejnili bezpečnostnú zraniteľnosť, ktorá spočíva v nedostatočnej implementácii bezpečnostných mechanizmov. Zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom TCP spojenia spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

31.05.2019

CVE

CVE-2018-15173

Zasiahnuté systémy

Nmap verzie staršie ako 7.70

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=60229
https://github.com/nmap/nmap/issues/1147
https://github.com/nmap/nmap/issues/1108
https://github.com/nmap/nmap/commit/ef385e5b7188eda72ba949bdd414ce14a9c6a7eb

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.8
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Emerson Ovation OCR400 Controller zraniteľnosti

Popis

Spoločnosť Emerson zverejnila informácie o bezpečnostných zraniteľnostiach vo svojom produkte Ovation OCR400. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov zasiahnutým systémom a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom špeciálne upravenej správy spôsobiť pretečenie zásobníka a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

28.05.2019

CVE

CVE-2019-10965, CVE-2019-10967

Zasiahnuté systémy

Emerson Ovation OCR400 Controller využívajúci Ovation Version s verziou staršou ako 3.3.1

Následky

Vykonanie škodlivého kódu
Eskalácia privilégií

Odporúčania

Administrátorom odporúčame zabezpečiť systém podľa návodu zverejnenom na:
https://ics-cert.us-cert.gov/advisories/ICSA-19-148-01
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-19-148-01
https://nvd.nist.gov/vuln/detail/CVE-2019-10967
https://nvd.nist.gov/vuln/detail/CVE-2019-10965

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

Identifikátor

AVEVA Vijeo Citect a CitectSCADA zraniteľnosť

Popis

Spoločnosť Aveva vydala bezpečnostné aktualizácie na svoje produkty Vijeo Citect a CitectSCADA. Zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

30.05.2019

CVE

CVE-2019-10981

Zasiahnuté systémy

Vijeo Citect verzie 7.30 a 7.40
CitetSCADA verzie 7.30 a 7.40

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-150-01
https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=51141

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.3
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Supra Smart Cloud TV zraniteľnosť

Popis

Bezpečnostní analytici zverejnili informácie o bezpečnostnej zraniteľnosti v Supra Smart Cloud TV. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonávať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

03.06.2019

CVE

CVE-2019-12477

Zasiahnuté systémy

Supra Smart Cloud TV

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
Administrátorom odporúčame bezodkladne aplikovať firewallové pravidlá a používať bezpečné prístupové heslo do WIFI siete.

Zdroje

https://sensorstechforum.com/cve-2019-12477-supra/
https://hackernews.blog/vulnerability-in-supra-smart-tvs-allows-you-to-display-any-video-on-the-screen/
https://www.theregister.co.uk/2019/06/04/supra_cloud_tv_flaw/