BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 11. 2018 - 13. 11. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

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-187

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.3
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť zdravotníckych pomôcok Roche Diagnostics Point of Care Handheld

Popis

Spoločnosť Roche Diagnostics informovala o viacerých zraniteľnostiach vo svojich produktoch Accu-Chek, CoaguChek a cobas.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom podvrhnutia špeciálne upravenej správy vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

06.11.2018

CVE

CVE-2018-18561, CVE-2018-18562, CVE-2018-18563, CVE-2018-18564, CVE-2018-18565

Zasiahnuté systémy

Accu-Chek Inform II všetky verzie staršie ako 03.06.00
CoaguChek Pro II všetky verzie staršie ako 04.03.00
CoaguChek XS Plus všetky verzie staršie ako 03.01.06
CoaguChek XS Pro všetky verzie staršie ako 03.01.06
cobas h 232 POC všetky verzie staršie ako 03.01.03 / 04.00.04

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup do systému

Odporúčania

Spoločnosť Roche Diagnostics by mala v mesiaci november 2018 vydať bezpečnostnú aktualizáciu na svoje produkty. Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSMA-18-310-01

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

Identifikátor

Zraniteľnosť Python Cryptographic Authority pyopenssl

Popis

Vývojári knižnice pyopenssl vydali bezpečnostné aktualizácie, ktoré opravujú viaceré zraniteľnosti. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nesprávnom spracovaní X.509 objektov a vzdialený neautentifikovaný útočník by ju mohol zneužiť na vykonanie ľubovoľného kódu alebo zneprístupnenie služby.

Dátum prvého zverejnenia varovania

08.11.2018

CVE

CVE-2018-1000807, CVE-2018-1000808

Zasiahnuté systémy

Pyopenssl, verzie 0.1.0, 0.2.0, 0.3.0, 0.4.0, 0.4.1, 0.5.0, 0.6.0, 0.7.0, 0.8.0, 0.9.0, 0.10.0, 0.11.0, 0.12.0, 0.13.0,1, 0.14.0, 0.15.0,1, 16.0.0, 16.1.0, 16.2.0, 17.0.0, 17.1.0, 17.2.0, 17.3.0, 17.4.0,

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59106
https://tools.cisco.com/security/center/viewAlert.x?alertId=59110

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

Identifikátor

Apache Hive zraniteľnosti

Popis

Spoločnosť Apache vydala bezpečnostné aktualizácie na svoj produkt Hive, ktoré opravujú bezpečnostné zraniteľností.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných opatrení a vzdialený autentifikovaný útočník by ich mohol zneužiť na získanie neoprávneného prístupu do cieleného systému.

Dátum prvého zverejnenia varovania

08.11.2018

CVE

CVE-2018-11777, CVE-2018-1314

Zasiahnuté systémy

Apache Hive všetky verzie staršie ako 2.3.4 a 3.1.1

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59108
https://tools.cisco.com/security/center/viewAlert.x?alertId=59109
https://lists.apache.org/thread.html/963c8e2516405c9b532b4add16c03b2c5db621e0c83e80f45049cbbb@%3Cdev.hive.apache.org%3E
https://lists.apache.org/thread.html/3da47dbcbf09697387f29d2f1aed970523b6b334d93afd3cced23727@%3Cdev.hive.apache.org%3E

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

Identifikátor

Apache Qpid zraniteľnosť

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt Qpid, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných opatrení a vzdialený neautentifikovaný útočník by ju mohol zneužiť na vykonanie útoku typu man-in-the-middle, čo má za následok neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

06.11.2018

CVE

CVE-2018-17187

Zasiahnuté systémy

Apache Qpid Proton-J verzia 0.3 až 0.29.0 (bezpečnostná záplata je vo verzii 0.30.0)

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/152832
https://seclists.org/oss-sec/2018/q4/148

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

Identifikátor

Zranitelnosti BIG-IP

Popis

Produkty BIG-IP od spoločnosti F5 obsahujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti sa nachádzajú v komponente TMM a vzdialený neautentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne vytvorených požiadaviek alebo sieťovej prevádzky mohol zneužiť na zneprístupnenie služby.
Ostatné zraniteľnosti by útočník mohol zneužiť na vykonanie neoprávnených zmien a tiež neoprávnený prístup k citlivým informáciám uložených v zasiahnutých systémoch.

Dátum prvého zverejnenia varovania

31.10.2018

CVE

CVE-2018-15317, CVE-2018-15318, CVE-2018-15319, CVE-2018-15320, CVE-2018-15321, CVE-2018-15322, CVE-2018-15323, CVE-2018-15324, CVE-2018-15325, CVE-2018-15326

Zasiahnuté systémy

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator) 14.x, 13.x, 12.x, 11.x
Enterprise Manager 3.x
BIG-IQ Centralized Management 5.x, 4.x
BIG-IQ Cloud and Orchestration 1.x
F5 iWorkflow 2.x

Bližšie informácie a konkrétne verzie zasiahnutých produktov môžete nájsť na odkazoch v časti Zdroje.

Následky

Zneprístupnenie služby, Neoprávnená zmena v systéme, Neoprávnený prístup k citlivým údajom

Odporúčania

Spoločnosť F5 priebežne vydáva aktualizácie na uvedené zraniteľnosti. Administrátorom odporúčame preveriť dostupnosť bezpečnostných záplat na stránkach výrobcu a následne vykonať aktualizáciu zasiahnutých systémov. V prípade, že záplaty nie sú dostupné, odporúčame sledovať stránky výrobcu a po ich vydaní vykonať aktualizáciu.

Zdroje
https://support.f5.com/csp/article/K43625118
https://support.f5.com/csp/article/K16248201
https://support.f5.com/csp/article/K64208870
https://support.f5.com/csp/article/K72442354
https://support.f5.com/csp/article/K01067037
https://support.f5.com/csp/article/K28003839
https://support.f5.com/csp/article/K26583415
https://support.f5.com/csp/article/K52206731
https://support.f5.com/csp/article/K77313277
https://support.f5.com/csp/article/K34652116

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.7
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť v produkte Cisco Advanced Malware Protection for Endpoints

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoj produkt Cisco Advanced Malware Protection for Endpoints, ktoré opravujú bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nesprávnej implementácii nahrávania dynamických knižníc DLL a lokálny autentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených DLL súborov mohol zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

29.10.2018

CVE

CVE-2018-15452

Zasiahnuté systémy

Cisco Advanced Malware Protection for Endpoints

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181029-amp-dll

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

Identifikátor

Zraniteľnosť Philips iSite a IntelliSpace PACS

Popis

Produkty iSite a IntelliSpace PACS od spoločnosti Philips obsahujú bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovan0mu útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente čiastočne narušiť dôvernosť, integritu a dostupnosť komponentu v systéme.

Dátum prvého zverejnenia varovania

08.11.2018

CVE

CVE-2018-17906

Zasiahnuté systémy

Philips iSite PACS, všetky verzie
Philips IntelliSpace PACS, všetky verzie

Následky

Neoprávnená zmena v systéme

Odporúčania

Spoločnosť Philips doposiaľ nevydala aktualizáciu zasiahnutých produktov. Produkt Philips iSite PACS je na konci svojej životnosti a nebudú preň už vydávané aktualizácie. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSMA-18-312-01

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

Identifikátor

Zraniteľnosť v PostgreSQL

Popis

Vývojári databázového systému PostgreSQL vydali aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému autentifikovanému útočníkovi vykonať SQL injekciu na zasiahnutom systéme.

Dátum prvého zverejnenia varovania

09.11.2018

CVE

CVE-2018-16850

Zasiahnuté systémy

postgresql-10 (PTS), verzie 10.0.0, 10.1.0, 10.2, 10.3.0, 10.4.0, 10.5.0, 11.0

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Následne odporúčame preveriť integritu databázy a prístupové logy na prítomnosť pokusov o SQL injekcie.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59117
https://www.postgresql.org/download/

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

Identifikátor

Nginx zraniteľnosti

Popis

Spoločnosť Nginx vydala aktualizáciu svojho produktu nginx, ktorá rieši viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v komponente ngx_http_mp4_module a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených MP4 súborov spôsobiť zneprístupnenie služieb na zasiahnutom systéme a tiež získať prístup k citlivým údajom.
Ostatné bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

06.11.2018

CVE

CVE-2018-16843, CVE-2018-16844, CVE-2018-16845

Zasiahnuté systémy

nginx verzie 1.0 až 1.15

Následky

Neoprávnený prístup k citlivým údajom, Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://mailman.nginx.org/pipermail/nginx-announce/2018/000221.html
http://mailman.nginx.org/pipermail/nginx-announce/2018/000220.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=59099
https://tools.cisco.com/security/center/viewAlert.x?alertId=59100
https://tools.cisco.com/security/center/viewAlert.x?alertId=59101