BEZPEČNOSTNÝ BULLETIN

Týždeň 03. 04. 2019 - 09. 04. 2019

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:
01380/2019/TS/OKB-104

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

Identifikátor

PostgreSQL zraniteľnosť

Popis

Bezpečnostní výskumníci objavili zraniteľnosť v databázovom systéme PostgreSQL.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.04.2019

CVE

CVE-2019-9193

Zasiahnuté systémy

PostgreSQL verzie 11.2 a staršie

Následky

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

Odporúčania

Na zraniteľnosť momentálne neexistuje záplata.
Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
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://tools.cisco.com/security/center/viewAlert.x?alertId=59916

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

Identifikátor

Libcomps zraniteľnosť

Popis

Vývojári Libcomps vydali aktualizáciu na svoj produkt, ktorá opravuje bezpečnostnú zraniteľnosť v comps_objmrtree_unite() funkcii.
Bezpečnostná zraniteľnosť je spôsobená nesprávnym spracovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.04.2019

CVE

CVE-2019-3817

Zasiahnuté systémy

Libcomps verzie staršie ako 0.1.10

Následky

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

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://github.com/rpm-software-management/libcomps/releases/tag/libcomps-0.1.10
https://tools.cisco.com/security/center/viewAlert.x?alertId=59872

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

Identifikátor

ZeroMQ libzmq zraniteľnosť

Popis

Vývojári ZeroMQ libzmq vydali aktualizáciu na svoj produkt, ktorá opravuje bezpečnostnú zraniteľnosť v zmq::v2_decoder_t::eight_byte_size_ready() funkcii.
Bezpečnostná zraniteľnosť je spôsobená nesprávnym spracovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.04.2019

CVE

CVE-2019-6250

Zasiahnuté systémy

ZeroMQ libzmq verzie staršie ako 4.3.1

Následky

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

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://github.com/zeromq/libzmq/releases/tag/v4.3.1/
https://tools.cisco.com/security/center/viewAlert.x?alertId=59871

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

Identifikátor

HPE Intelligent Management Center viacero zraniteľností

Popis

Bezpečnosnti výskumníci objavili viacero bezpečnostných zraniteľností v produkte HPE Intelligent Management Center.
Všetky tieto bezpečnostné zraniteľnosti sú spôsobené nesprávnym spracovaním používateľských vstupov a umožňujú vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.04.2019

CVE

-

Zasiahnuté systémy

HPE Intelligent Management Center

Následky

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

Odporúčania

Na zraniteľnosť momentálne neexistuje záplata.
Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
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://exchange.xforce.ibmcloud.com/vulnerabilities/159135
https://exchange.xforce.ibmcloud.com/vulnerabilities/159136
https://exchange.xforce.ibmcloud.com/vulnerabilities/159137
https://exchange.xforce.ibmcloud.com/vulnerabilities/159138
https://exchange.xforce.ibmcloud.com/vulnerabilities/159139
https://exchange.xforce.ibmcloud.com/vulnerabilities/159140
https://exchange.xforce.ibmcloud.com/vulnerabilities/159141
https://exchange.xforce.ibmcloud.com/vulnerabilities/159142
https://exchange.xforce.ibmcloud.com/vulnerabilities/159143
https://exchange.xforce.ibmcloud.com/vulnerabilities/159144

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

Identifikátor

Dell EMC IsilonSD Management Server viacero zraniteľností

Popis

Spoločnosť Dell vydala aktualizáciu na svoj produkt EMC IsilonSD Management Server, ktorá opravuje viacero bezpečnostných zraniteľností.
Obe bezpečnostné zraniteľnosti sú spôsobene nesprávnym spracovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať Cross-Site Scripting (XSS) útok.

Dátum prvého zverejnenia varovania

04.04.2019

CVE

CVE-2019-3708, CVE-2019-3709

Zasiahnuté systémy

Dell EMC IsilonSD Management Server staršie ako 1.1.1

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://seclists.org/fulldisclosure/2019/Apr/5
https://exchange.xforce.ibmcloud.com/vulnerabilities/159133
https://exchange.xforce.ibmcloud.com/vulnerabilities/159134

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache HTTP Server zraniteľnosť

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj HTTP server, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

03.04.2019

CVE

CVE-2019-0211

Zasiahnuté systémy

Apache HTTP Server verzie staršie ako 2.4.39

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2019-0211
https://www.helpnetsecurity.com/2019/04/03/apache-web-server-cve-2019-0211/
https://access.redhat.com/security/cve/cve-2019-0211

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

TianoCore EDK II viacero zraniteľností

Popis

Vývojári TianoCore EDK II vydali aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností. Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégia a získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

02.04.2019

CVE

CVE-2018-12178, CVE-2018-12179, CVE-2018-12180, CVE-2018-12181, CVE-2018-12182, CVE-2018-12183

Zasiahnuté systémy

TianoCore EDK II

Následky

Eskalácia privilégií
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://tools.cisco.com/security/center/viewAlert.x?alertId=59890
https://tools.cisco.com/security/center/viewAlert.x?alertId=59891
https://tools.cisco.com/security/center/viewAlert.x?alertId=59892
https://tools.cisco.com/security/center/viewAlert.x?alertId=59893
https://tools.cisco.com/security/center/viewAlert.x?alertId=59894
https://tools.cisco.com/security/center/viewAlert.x?alertId=59895

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

Identifikátor

Adobe Acrobat a Adobe Reader zraniteľnosť

Popis

Spoločnosť Adobe vydala aktualizácie na svoje produkty Acrobat a Acrobat Reader, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nesprávnym spracovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.04.2019

CVE

CVE-2019-7131

Zasiahnuté systémy

Adobe Acrobat a Reader verzie staršie ako 2017 2017.011.30113, DC 2015.006.30464, 2019.010.20069

Následky

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

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://helpx.adobe.com/security/products/acrobat/apsb19-02.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/158935

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

Identifikátor

Eclipse viacero zraniteľností

Popis

Vývojári IDE Eclipse vydali bezpečnostné aktualizácie na knižnice Mosquitto a Jetty, ktoré opravujú bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti sú spôsobené nesprávnym spracovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

04.04.2019

CVE

CVE-2017-7655, CVE-2018-12545

Zasiahnuté systémy

Eclipse Mosquitto verzie staršie ako 1.5
Eclipse Jetty verzie staršie ako 9.3.25.v20180904 a 9.4.12.v20180830

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://github.com/eclipse/mosquitto/releases/tag/v1.5
https://github.com/eclipse/jetty.project/releases
https://tools.cisco.com/security/center/viewAlert.x?alertId=59899
https://tools.cisco.com/security/center/viewAlert.x?alertId=59889

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

Identifikátor

Lupus Electronics XT2 Plus viacero zraniteľností

Popis

Spoločnosť Lupus Electronics vydala aktualizáciu na svoje poplašné zariadenia XT2 Plus, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

04.04.2019

CVE

-

Zasiahnuté systémy

XT2 Plus verzie staršie ako 0.0.3.0

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://exchange.xforce.ibmcloud.com/vulnerabilities/159043
https://exchange.xforce.ibmcloud.com/vulnerabilities/159044
https://exchange.xforce.ibmcloud.com/vulnerabilities/159045
https://exchange.xforce.ibmcloud.com/vulnerabilities/159046

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

Identifikátor

Splunk Python SDK zraniteľnosť

Popis

Vývojári Splunk Python SDK vydali aktualizáciu na svoj produkt, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

02.04.2019

CVE

CVE-2019-5729

Zasiahnuté systémy

Splunk Python SDK verzie staršie ako 1.6.6

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://github.com/splunk/splunk-sdk-python/releases
https://tools.cisco.com/security/center/viewAlert.x?alertId=59875