BEZPEČNOSTNÝ BULLETIN

Týždeň 30. 01. 2019 - 05. 02. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Mozilla Firefox viacero zraniteľností	Vysoká	**8.8**
02.	Google Chrome viacero zraniteľností	Vysoká	**8.8**
03.	Aveva Wonderware zraniteľnosť	Vysoká	**8.8**
04.	Mozilla Thunderbird viacero zraniteľností	Vysoká	**8.8**
05.	ACD Systems Canvas Draw 5 viacero zraniteľností	Vysoká	**8.8**
06.	Wecon LeviStudioU viacero zraniteľností	Vysoká	**8.8**
07.	Bitdefender SafePay zraniteľnosti	Vysoká	**8.8**
08.	OpenOffice a LibreOffice zraniteľnosť	Vysoká	**8.8**
09.	Yokogawa License Manager Service zraniteľnosť	Vysoká	**8.1**
10.	Keybase for macOS zraniteľnosť	Vysoká	**7.8**
11.	Mitsubishi Electric MELSEC-Q Series PLCs zraniteľnosť	Vysoká	**7.5**
12.	Zraniteľnosť sieťových zariadení Ubiquiti	Vysoká	**7.5**
13.	SolarWinds Serv-U FTP server zraniteľnosť	Vysoká	**7.2**
14.	IBM Security Identity Manager zraniteľnosť	Vysoká	**7.2**
15.	Becton, Dickinson and Company (BD) FACSLyric zraniteľnosť	Stredná	**6.8**

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-033

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

Identifikátor

Mozilla Firefox viacero zraniteľností

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v internetových prehliadačoch Firefox a Firefox ESR.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód na zraniteľnom systéme.

Dátum prvého zverejnenia varovania

29.01.2019

CVE

CVE-2011-3079, CVE-2018-18500, CVE-2018-18501, CVE-2018-18502, CVE-2018-18503, CVE-2018-18504, CVE-2018-18505, CVE-2018-18506,

Zasiahnuté systémy

Mozilla Firefox verzie staršie ako 65
Mozilla Firefox ESR verzie staršie ako 60.5

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2019-02/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-01/

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

Identifikátor

Google Chrome viacero zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu, ktorá opravuje viacero chýb a 58 bezpečnostných zraniteľností v internetovom prehliadači Chrome.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód na zraniteľnom systéme.

Dátum prvého zverejnenia varovania

29.01.2019

CVE

CVE-2019-5754, CVE-2019-5755, CVE-2019-5756, CVE-2019-5757, CVE-2019-5758, CVE-2019-5759, CVE-2019-5760, CVE-2019-5761, CVE-2019-5762, CVE-2019-5763, CVE-2019-5764, CVE-2019-5765, CVE-2019-5766, CVE-2019-5767, CVE-2019-5768, CVE-2019-5769, CVE-2019-5770, CVE-2019-5771, CVE-2019-5772, CVE-2019-5773, CVE-2019-5774, CVE-2019-5775, CVE-2019-5776, CVE-2019-5777, CVE-2019-5778, CVE-2019-5779, CVE-2019-5780, CVE-2019-5781, CVE-2019-5782

Zasiahnuté systémy

Google Chrome verzie staršie ako 72.0.3626.81

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://chromereleases.googleblog.com/2019/01/stable-channel-update-for-desktop.html

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

Identifikátor

Aveva Wonderware zraniteľnosť

Popis

Spoločnosť Aveva vydala bezpečnostnú aktualizáciu na svoj produkt Wonderware System Platform, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciu bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom API rozhrania eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

24.01.2019

CVE

CVE-2019-6525

Zasiahnuté systémy

Aveva Wonderware System Platform 2017 verzie staršie ako Update 3

Následky

Eskalácia privilégií

Odporúčania

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

Zdroje

https://sw.aveva.com/hubfs/assets-2018/pdf/security-bulletin/SecurityBulletin_LFSec135.pdf
https://ics-cert.us-cert.gov/advisories/ICSA-19-029-03

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

Identifikátor

Mozilla Thunderbird viacero zraniteľností

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v e-mailovom klientovi Thunderbird.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód na napadnutom systéme.

Dátum prvého zverejnenia varovania

29.01.2019

CVE

CVE-2011-3079, CVE-2016-5824, CVE-2018-18500, CVE-2018-18501, CVE-2018-18505

Zasiahnuté systémy

Mozilla Thunderbird verzie staršie ako 60.5

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2019-03/
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-mozilla-thunderbird-could-allow-for-arbitrary-code-execution_2019-012/

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

Identifikátor

ACD Systems Canvas Draw 5 viacero zraniteľností

Popis

Spoločnosť ACD Systems vydala bezpečnostnú aktualizáciu na svoj produkt Canvas Draw 5, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia upravených TIFF a CAL súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.01.2019

CVE

CVE-2018-3981, CVE-2018-3976, CVE-2018-3973, CVE-2018-3980

Zasiahnuté systémy

ACDSystems Canvas Draw verzie staršie ako 5.0.1

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0648
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0638
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0642
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0649

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

Identifikátor

Wecon LeviStudioU viacero zraniteľností

Popis

Bezpečnostné výskumníci informovali o viacerých zraniteľnostiach v produkte Wecon LeviStudioU. Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.01.2019

CVE

-

Zasiahnuté systémy

Wecon LeviStudioU

Následky

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

Odporúčania

Spoločnosť Wecon doposiaľ nevydala aktualizáciu svojho produktu. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu. Tiež odporúčame aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL). Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-19-156/
https://www.zerodayinitiative.com/advisories/ZDI-19-155/
https://www.zerodayinitiative.com/advisories/ZDI-19-154/
https://www.zerodayinitiative.com/advisories/ZDI-19-153/
https://www.zerodayinitiative.com/advisories/ZDI-19-152/
https://www.zerodayinitiative.com/advisories/ZDI-19-151/
https://www.zerodayinitiative.com/advisories/ZDI-19-150/
https://www.zerodayinitiative.com/advisories/ZDI-19-149/
https://www.zerodayinitiative.com/advisories/ZDI-19-147/
https://www.zerodayinitiative.com/advisories/ZDI-19-148/
https://www.zerodayinitiative.com/advisories/ZDI-19-146/
https://www.zerodayinitiative.com/advisories/ZDI-19-145/
https://www.zerodayinitiative.com/advisories/ZDI-19-144/
https://www.zerodayinitiative.com/advisories/ZDI-19-143/

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

Identifikátor

Bitdefender SafePay zraniteľnosti

Popis

Spoločnosť Bitdefender vydala bezpečnostnú aktualizáciu na svoj produkt Bitdefender SafePay, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov pri spracovaní TIScript súborov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia upravených TIScript súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.01.2019

CVE

CVE-2019-6738, CVE-2019-6737, CVE-2019-6736

Zasiahnuté systémy

Bitdefender SafePay verzie staršie ako 23.0.11.44

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-19-157/
https://www.zerodayinitiative.com/advisories/ZDI-19-158/
https://www.zerodayinitiative.com/advisories/ZDI-19-159/

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

Identifikátor

OpenOffice a LibreOffice zraniteľnosť

Popis

Bezpečnostný výskumník informoval o zraniteľnosti v kancelárskych balíkoch OpenOffice a LibreOffice. Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného ODT dokumentu vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

01.02.2019

CVE

CVE-2018-16858

Zasiahnuté systémy

OpenOffice
LibreOffice verzie staršie ako 6.0.7 a 6.1.3

Následky

Vykonanie škodlivého kódu

Odporúčania

Vývojári balíka OpenOffice doposiaľ nevydali aktualizáciu svojho produktu. Používateľom balíka OpenOffice odporúčame premenovať alebo odstrániť súbor pythonscript.py z inštalačnej zložky. Administrátorom balíka LibreOffice odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy a súbory z neznámych zdrojov.

Zdroje

https://insert-script.blogspot.com/2019/02/libreoffice-cve-2018-16858-remote-code.html
https://www.libreoffice.org/about-us/security/advisories/cve-2018-16858/
https://www.theregister.co.uk/AMP/2019/02/04/apache_openoffice_no_patch

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

Identifikátor

Yokogawa License Manager Service zraniteľnosť

Popis

Spoločnosť Yokogawa vydala bezpečnostnú aktualizáciu na svoj produkt License Manager Service, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciu bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

25.01.2019

CVE

CVE-2019-5909

Zasiahnuté systémy

Yokogawa License Manager Service CENTUM VP (R5.01.00 - R6.06.00), CENTUM VP Entry Class (R5.01.00 - R6.06.00), ProSafe-RS (R3.01.00 - R4.04.00), PRM (R4.01.00 – R4.02.00) a B/M9000 VP (R7.01.01 - R8.02.03)

Následky

Vykonanie škodlivého kódu

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-19-029-01

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

Identifikátor

Keybase for macOS zraniteľnosť

Popis

Vývojári komunikačnej aplikácie Keybase vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciu bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

28.12.2018

CVE

CVE-2019-7249

Zasiahnuté systémy

Keybase for macOS verzie staršie ako 2.12.6

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/156491
https://hackerone.com/reports/471739

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

Identifikátor

Mitsubishi Electric MELSEC-Q Series PLCs zraniteľnosť

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostnú aktualizáciu na svoje produkty MELSEC-Q PLC, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania paketov na porte 5007 spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

29.01.2019

CVE

CVE-2019-6535

Zasiahnuté systémy

Mitsubishi Electric MELSEC-Q Q03/04/06/13/26UDVCPU: serial number 20081 a staršie
Q04/06/13/26UDPVCPU: serial number 20081 a staršie
Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 a staršie

Následky

Zneprístupnenie služby

Odporúčania

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

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-029-02

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

Identifikátor

Zraniteľnosť sieťových zariadení Ubiquiti

Popis

Bezpečnostní výskumníci informovali o zraniteľnosti v sieťových zariadeniach Ubiquiti používajúcich firmvér airOS. Bezpečnostná zraniteľnosť spočíva v dostupnosti portu UDP/TCP 10001 z internetu a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonávať amplifikačné DDoS útoky.

Dátum prvého zverejnenia varovania

29.01.2019

CVE

-

Zasiahnuté systémy

Sieťové zariadenia Ubiquiti používajúce airOS (NanoStation, AirGrid, LiteBeam, PowerBeam, NanoBeam, NanoBridge, miMo, LiteAP, EdgeRouter, Bullet, Rocket, mFi, BaseStation, PowerStation, EdgeSwitch, AirFiber, AirCam, UniFi AP, Wave AC a ďalšie)

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame aplikovať firewallové pravidlá a blokovať port UDP/TCP 10001.
Spoločnosť Ubiquiti Networks doposiaľ nevydala bezpečnostnú aktualizáciu. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu. Taktiež odporúčame zmeniť predvolené autentifikačné údaje zariadenia.

Zdroje

https://blog.rapid7.com/2019/02/01/ubiquiti-discovery-service-exposures/
https://community.ubnt.com/t5/EdgeRouter/UDP-broadcasts-on-port-10001/td-p/461223
https://www.securityweek.com/flaw-possibly-affecting-500000-ubiquity-devices-exploited-wild
https://community.ubnt.com/t5/airMAX-General-Discussion/airOS-airMAX-and-management-access/m-p/2654023

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SolarWinds Serv-U FTP server zraniteľnosť

Popis

Vývojári FTP servera Serv-U vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť vo funkcii importu CSV súborov.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom podvrhnutia
upravených CSV súborov eskalovať svoje privilégiá na zraniteľnom systéme.

Dátum prvého zverejnenia varovania

31.01.2019

CVE

CVE-2018-15906

Zasiahnuté systémy

SolarWinds Serv-U verzie staršie ako 15.1.6 Hotfix 2

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://seclists.org/fulldisclosure/2019/Feb/4
https://exchange.xforce.ibmcloud.com/vulnerabilities/156546

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

IBM Security Identity Manager zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Security Identity Manager, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciu bezpečnostných mechanizmov a umožňuje autentifikovanému útočníkovi s fyzickým prístupom k systému obísť bezpečnostné mechanizmy a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

29.01.2019

CVE

CVE-2019-4038

Zasiahnuté systémy

IBM Security Identity Manager verzie staršie ako 6.0.0.21 a 7.0.1.11

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www-01.ibm.com/support/docview.wss?uid=ibm10869604
https://exchange.xforce.ibmcloud.com/vulnerabilities/156162

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

Identifikátor

Becton, Dickinson and Company (BD) FACSLyric zraniteľnosť

Popis

Spoločnosť BD informuje o bezpečnostnej zraniteľnosti vo svojom produkte FACSLyric.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciu bezpečnostných mechanizmov a umožňuje útočníkovi s fyzickým prístupom ku zariadeniu získať neoprávnený administrátorský prístup do systému.

Dátum prvého zverejnenia varovania

29.01.2019

CVE

CVE-2019-6517

Zasiahnuté systémy

BD FACSLyric Research Use Only, Windows 10 Professional Operating System, U.S. and Malaysian verzie vydané medzi novembrom 2017 a novembrom 2018
BD FACSLyric IVD Windows 10 Professional Operating System U.S. release

Následky

Neoprávnený prístup do systému

Odporúčania

Odporúčame limitovať fyzický prístup ku zraniteľným zariadeniam. Odporúčame tiež kontaktovať dodávateľa zraniteľných systémov, ktorý zraniteľnosť odstráni.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSMA-19-029-02