BEZPEČNOSTNÝ BULLETIN

Týždeň 13. 03. 2019 - 19. 03. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome viacero zraniteľností	Vysoká	**8.8**
02.	Adobe Photoshop CC zraniteľnosť	Vysoká	**8.8**
03.	Zraniteľnosti produktov Lenovo	Vysoká	**8.4**
04.	Intel CSME, Server Platform Services, Trusted Execution Engine a Intel Active Management Technology viacero zraniteľností	Vysoká	**8.2**
05.	Intel Graphics Driver zraniteľnosti	Vysoká	**8.2**
06.	HashiCorp Consul zraniteľnosť	Vysoká	**8.1**
07.	LCDS LAquis SCADA zraniteľnosť	Vysoká	**7.8**
08.	VMware zraniteľnosť	Vysoká	**7.8**
09.	Openwsman opwnswand zraniteľnosť	Vysoká	**7.5**
10.	Zraniteľnosť bezdrôtovej klávesnice Fujitsu Set LX901	Vysoká	**7.5**
11.	Zraniteľnosť Video modulu pre Drupal	Vysoká	**7.2**
12.	CleanMyMac X zraniteľnosť	Vysoká	**7.1**
13.	Gemalto Sentinel UltraPro	Stredná	**6.5**
14.	VideoXpert OpsCenter zraniteľnosť	Stredná	**6.4**

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-084

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 60 bezpečnostných zraniteľností v internetovom prehliadači Chrome. Najzávažnejšie zraniteľnosti 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

12.03.2019

CVE

CVE-2019-5788, CVE-2019-5789, CVE-2019-5790, CVE-2019-5791, CVE-2019-5792, CVE-2019-5793, CVE-2019-5794, CVE-2019-5795, CVE-2019-5796, CVE-2019-5797, CVE-2019-5798, CVE-2019-5799, CVE-2019-5800, CVE-2019-5801, CVE-2019-5802, CVE-2019-5803, CVE-2019-5804

Zasiahnuté systémy

Google Chrome verzie staršie ako 73.0.3683.75

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby nenavštevovali nedôveryhodné webové stránky.
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://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2019-030/
https://chromereleases.googleblog.com/2019/03/stable-channel-update-for-desktop_12.html

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

Identifikátor

Adobe Photoshop CC zraniteľnosť

Popis

Spoločnosť Adobe vydala bezpečnostnú aktualizáciu na svoj produkt Photoshop CC, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov pri parsovaní GIF súborov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.03.2019

CVE

CVE-2019-7094

Zasiahnuté systémy

Adobe Photoshop CC staršie ako 19.1.8
Photoshop CC staršie ako 20.0.4

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali súbory z neznámych zdrojov.
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://www.zerodayinitiative.com/advisories/ZDI-19-258/
https://www.cisecurity.org/advisory/a-vulnerability-in-adobe-photoshop-cc-could-allow-for-arbitrary-code-execution-apsb19-15_2019-028/
https://helpx.adobe.com/security/products/photoshop/apsb19-15.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosti produktov Lenovo

Popis

Spoločnosť Lenovo vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností v TianoCore EDK II BIOSe.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme alebo spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

14.03.2019

CVE

-

Zasiahnuté systémy

Lenovo IdeaCentre, QITIAN, IdeaPad, ThinkCentre, YANGTIAN, ThinkPad, ThinkServer, ThinkServer, ThinkStation, ThinkSystem

Následky

Eskalácia privilégií
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.lenovo.com/sk/en/solutions/len-22660
https://exchange.xforce.ibmcloud.com/vulnerabilities/158190

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

Identifikátor

Intel CSME, Server Platform Services, Trusted Execution Engine a Intel Active Management Technology viacero zraniteľností

Popis

Spoločnosť Intel vydala bezpečnostné aktualizácie na svoje produkty Intel CSME, Server Platform Services, Trusted Execution Engine a Intel Active Management Technology, ktoré opravujú viacero bezpečnostných zraniteľností. Najzávažnejšie zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.03.2019

CVE

CVE-2018-12185, CVE-2018-12187, CVE-2018-12188, CVE-2018-12189, CVE-2018-12190, CVE-2018-12191, CVE-2018-12192, CVE-2018-12196, CVE-2018-12198, CVE-2018-12199, CVE-2018-12200

Zasiahnuté systémy

Intel CSME verzie staršie ako 11.8.60, 11.11.60, 11.22.60 a 12.0.20
Intel Server Platform Services verzie staršie ako 4.00.04.383 a 4.01.02.174
Intel Trusted Execution Engine verzie staršie ako 3.1.60 a 4.0.10

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://exchange.xforce.ibmcloud.com/vulnerabilities/158180
https://support.lenovo.com/sk/en/solutions/len-25083
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00185.html

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

Identifikátor

Intel Graphics Driver zraniteľnosti

Popis

Spoločnosť Intel vydala bezpečnostné aktualizácie na svoj produkt Intel Graphics Driver, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov v komponente Kernel Mode Driver a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.03.2019

CVE

CVE-2018-12209, CVE-2018-12210, CVE-2018-12211, CVE-2018-12212, CVE-2018-12213, CVE-2018-12214, CVE-2018-12215, CVE-2018-12216, CVE-2018-12217, CVE-2018-12218, CVE-2018-12219, CVE-2018-12220, CVE-2018-12221, CVE-2018-12222, CVE-2018-12223, CVE-2018-12224, CVE-2018-18089, CVE-2018-18090, CVE-2018-18091

Zasiahnuté systémy

Intel Graphics Driver pre Windows verzie staršie ako 10.18.x.5059 (15.33.x.5059), 10.18.x.5057 (15.36.x.5057), 20.19.x.5063 (15.40.x.5063), 21.20.x.5064 (15.45.x.5064) a 24.20.100.6373

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://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00189.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/158152

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

Identifikátor

HashiCorp Consul zraniteľnosť

Popis

Spoločnosť HashiCorp vydala bezpečnostnú aktualizáciu na svoj produkt Consul, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi eskalovať svoje privilégia.

Dátum prvého zverejnenia varovania

18.03.2019

CVE

CVE-2019-8336

Zasiahnuté systémy

HashiCorp Consul verzie staršie ako 1.4.3

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://github.com/hashicorp/consul/releases
https://tools.cisco.com/security/center/viewAlert.x?alertId=59796

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

Identifikátor

LCDS LAquis SCADA zraniteľnosť

Popis

Spoločnosť LCDS vydala bezpečnostnú aktualizáciu na svoj produkty LAquis SCADA, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených ELS súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.03.2019

CVE

CVE-2019-6536

Zasiahnuté systémy

LAquis SCADA verzie staršie ako 4.3.1.71

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
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://ics-cert.us-cert.gov/advisories/ICSA-19-073-01

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

Identifikátor

VMware zraniteľnosť

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na svoj produkt VMware Workstation, ktoré opravujú bezpečnostnú zraniteľnosť.
Zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

14.03.2019

CVE

CVE-2019-5511, CVE-2019-5512

Zasiahnuté systémy

VMware Workstation verzie staršie ako 14.1.6
VMware Workstation verzie staršie ako 15.0.3

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2019-0002.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/158216

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

Identifikátor

Openwsman opwnswand zraniteľnosť

Popis

Nástroj Openwsman obsahuje viacero zraniteľností, ktoré spočívajú v nedostatočnej implementácií bezpečnostných mechanizmov v opwnswand Daemone. Najzávažnejšia zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravenej HTTP požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

15.03.2019

CVE

CVE-2019-3816, CVE-2019-3833

Zasiahnuté systémy

Openwsman 2.2 až 2.6

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Vývojári Openwsman zatiaľ nevydali aktualizáciu riešiacu uvedenú zraniteľnosť.
Administrátorom odporúčame sledovať stránky vývojárov a po vydaní bezpečnostných záplat vykonať aktualizáciu.
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=59786
https://tools.cisco.com/security/center/viewAlert.x?alertId=59785

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

Identifikátor

Zraniteľnosť bezdrôtovej klávesnice Fujitsu Set LX901

Popis

Bezpečnostní výskumníci objavili zraniteľnosť v bezdrôtovej klávesnici Fujitsu Set LX901. Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému útočníkovi, nachádzajúcemu sa v dosahu bezdrôtového prijímača, prostredníctvom zasielania špeciálne upravených paketov prevziať kontrolu nad klávesnicou.

Dátum prvého zverejnenia varovania

15.03.2019

CVE

CVE-2019-9835

Zasiahnuté systémy

Bezdrôtová klávesnica Fujitsu Set LX901

Následky

Neoprávnený prístup do systému

Odporúčania

V súčasnej dobe na zraniteľnosť neexistuje bezpečnostná záplata. Až do vydania aktualizácie odporúčame používať iný model klávesnice.

Zdroje

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2018-033.txt
https://exchange.xforce.ibmcloud.com/vulnerabilities/158235

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

Identifikátor

Zraniteľnosť Video modulu pre Drupal

Popis

Vývojári redakčného systému Drupal vydali bezpečnostnú aktualizáciu Video modulu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov v administrátorských formulároch a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených požiadaviek vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.03.2019

CVE

Zasiahnuté systémy

Video modul pre Drupal 7.x, verzie staršie ako 7.x-2.14

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Drupal so zraniteľnou verziou modulu Video. V prípade že áno, zabezpečte aktualizáciu redakčného systému a modulu.
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://www.drupal.org/sa-contrib-2019-037
https://exchange.xforce.ibmcloud.com/vulnerabilities/158168

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

Identifikátor

CleanMyMac X zraniteľnosť

Popis

Spoločnosť MacPaw vydala bezpečnostnú aktualizáciu na svoj produkt Clean My Mac X, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi uskutočniť neoprávnené zmeny v systéme a eskalovať svoje privilégia.

Dátum prvého zverejnenia varovania

15.01.2019

CVE

CVE-2019-5011

Zasiahnuté systémy

Clean My Mac X verzie staršie ako 4.30

Následky

Neoprávnená zmena v systéme
Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.talosintelligence.com/vulnerability_reports/TALOS-2019-0759

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

Identifikátor

Gemalto Sentinel UltraPro

Popis

Spoločnosť Gemalto vydala bezpečnostnú aktualizáciu na svoj produkt Sentinel UltraPro, ktorá opravuje bezpečnostnú zraniteľnosť v knižnici ux32w.dll.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.03.2019

CVE

CVE-2019-6534

Zasiahnuté systémy

Gemalto Sentinel UltraPro verzie staršie ako 1.3.3

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://ics-cert.us-cert.gov/advisories/ICSA-19-073-02

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.4
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

VideoXpert OpsCenter zraniteľnosť

Popis

Spoločnosť Pelco vydala bezpečnostnú aktualizáciu na svoj produkt VideoXpert OpsCenter, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.03.2019

CVE

CVE-2018-7840

Zasiahnuté systémy

VideoXpert OpsCenter verzie staršie ako 3.1

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
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://www.schneider-electric.com/en/download/document/SEVD-2019-071-01/