BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 08. 2019 - 13. 08. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome viacero zraniteľností	Vysoká	**8.8**
02.	Jenkins plugins viacero zraniteľností	Vysoká	**8.8**
03.	Zraniteľnosti Canon EOS a PowerShot fotoaparátov	Vysoká	**8.8**
04.	Zraniteľnosti v produktoch Adobe	Vysoká	**8.8**
05.	Zraniteľnosť v prepínačoch Siemens SCALANCE X	Vysoká	**8.6**
06.	OSIsoft PI Web API Zraniteľnosti	Vysoká	**8.5**
07.	Valve Steam game client zraniteľnosť	Vysoká	**8.2**
08.	Intel Zraniteľnosti	Vysoká	**8.2**
09.	Kubernetes zraniteľnosti	Vysoká	**8.1**
10.	Delta Industrial Automation DOPSoft Zraniteľnosti	Vysoká	**7.8**
11.	Zraniteľnosti v produktoch Siemens SIPROTEC 5 a DIGSI 5	Vysoká	**7.5**
12.	Zraniteľnosti v produktoch Apache Solr a Apache Spark	Vysoká	**7.2**
13.	Zraniteľnosti v produktoch Siemens SCALANCE	Stredná	**6.6**

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-205

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 aktualizáciu na svoj internetový prehliadač Google Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
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

06.08.2019

CVE

CVE-2019-5867, CVE-2019-5868

Zasiahnuté systémy

Google Chrome verzie staršie ako 76.0.3809.100

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 neoverené e-mailové správy, prílohy z neznámych zdrojov a 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://chromereleases.googleblog.com/2019/08/stable-channel-update-for-desktop.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2019-079/

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 informovali o bezpečnostných zraniteľnostiach vo viacerých zásuvných moduloch.
Najvážnejšia bezpečnostná zraniteľnosť v Simple Travis Pipeline Runner Plugin je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.08.2019

CVE

CVE-2019-10367, CVE-2019-10368, CVE-2019-10369, CVE-2019-10370, CVE-2019-10371, CVE-2019-10372, CVE-2019-10373, CVE-2019-10374, CVE-2019-10375, CVE-2019-10376, CVE-2019-10377, CVE-2019-10378, CVE-2019-10379, CVE-2019-10380, CVE-2019-10381, CVE-2019-10382, CVE-2019-10385, CVE-2019-10386, CVE-2019-10387, CVE-2019-10388, CVE-2019-10389

Zasiahnuté systémy

Configuration as Code Plugin verzie staršie ako 1.27
JClouds Plugin verzie staršie ako 2.15
Avatar Plugin verzia 1.2 a staršie
Build Pipeline Plugin verzia 1.5.8 a staršie
Codefresh Integration Plugin verzia 1.8 a staršie
Configuration as Code Plugin verzia 1.26 a staršie
eggPlant Plugin verzia 2.2 a staršie
File System SCM Plugin verzia 2.1 a staršie
Google Cloud Messaging Notification Plugin verzia 1.0 a staršie
Gitlab Authentication Plugin verzia 1.4 a staršie
JClouds Plugin verzia 2.14 a staršie
Mask Passwords Plugin verzia 2.12.0 a staršie
PegDown Formatter Plugin verzia 1.3 a staršie
Relution Enterprise Appstore Publisher Plugin verzia 1.24 a staršie
Simple Travis Pipeline Runner Plugin verzia 1.0 a staršie
TestLink Plugin verzia 3.16 a staršie
VMware Lab Manager Slaves Plugin verzia 0.2.8 a staršie
Wall Display Master Project Plugin verzia 0.6.34 a staršie
XL TestView Plugin verzia 1.2.0 a staršie

Následky

Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému

Odporúčania
Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. V prípade pluginov, na ktoré doposiaľ neboli vydané aktualizácie administrátorom odporúčame zvážiť ich odinštalovanie a tiež sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje
https://jenkins.io/security/advisory/2019-08-07/ https://exchange.xforce.ibmcloud.com/vulnerabilities/164954

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

Identifikátor

Zraniteľnosti Canon EOS a PowerShot fotoaparátov

Popis

Spoločnosť Canon informovala o bezpečnostných zraniteľnostiach vo fotoaparátoch rady EOS a PowerShot.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov v PTP (Picture Transfer Protocol) a umožňujú vzdialenému, neautentifikovanému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente, spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.08.2019

CVE

CVE-2019-5994, CVE-2019-5995, CVE-2019-5998, CVE-2019-5999, CVE-2019-6000, CVE-2019-6001

Zasiahnuté systémy

Canon EOS Series
Canon EOS 80D verzie staršie ako 1.0.3
Canon PowerShot SX70HS
Canon PowerShot SX740HS
Canon PowerShot G5XMarkII

Následky

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

Odporúčania

Spoločnosť Canon doposiaľ vydala aktualizáciu iba na model Canon EOS 80D. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
Používateľom odporúčame zapínať sieťové funkcie v zariadeniach iba na nevyhnutne potrebný čas a nepripájať fotoaparáty ku nedôveryhodných zariadeniam a WIFI sieťam.
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

http://jvn.jp/en/vu/JVNVU97511331/index.html
https://www.canon-europe.com/support/product-security/
https://www.usa.canon.com/internet/portal/us/home/support/product-advisories/detail/the-vulnerability-in-canon-digital-cameras

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

Identifikátor

Zraniteľnosti v produktoch Adobe

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostné zraniteľnosti v produktoch Adobe After Effects CC, Character Animator CC, Premiere Pro CC, Prelude CC, Creative Cloud Desktop Application, Acrobat a Reader, Experience Manager a Photoshop CC.
Najzávažnejšie zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.08.2019

CVE

CVE-2019-7832, CVE-2019-7870, CVE-2019-7931, CVE-2019-7957, CVE-2019-7958, CVE-2019-7959,
CVE-2019-7961, CVE-2019-7964, CVE-2019-7965, CVE-2019-7968, CVE-2019-7969, CVE-2019-7970,
CVE-2019-7971, CVE-2019-7972, CVE-2019-7973, CVE-2019-7974, CVE-2019-7975, CVE-2019-7976,
CVE-2019-7977, CVE-2019-7978, CVE-2019-7979, CVE-2019-7980, CVE-2019-7981, CVE-2019-7982,
CVE-2019-7983, CVE-2019-7984, CVE-2019-7985, CVE-2019-7986, CVE-2019-7987, CVE-2019-7988,
CVE-2019-7989, CVE-2019-7990, CVE-2019-7991, CVE-2019-7992, CVE-2019-7993, CVE-2019-7994,
CVE-2019-7995, CVE-2019-7996, CVE-2019-7997, CVE-2019-7998, CVE-2019-7999, CVE-2019-8000,
CVE-2019-8001, CVE-2019-8002, CVE-2019-8003, CVE-2019-8004, CVE-2019-8005, CVE-2019-8006,
CVE-2019-8007, CVE-2019-8008, CVE-2019-8009, CVE-2019-8010, CVE-2019-8011, CVE-2019-8012,
CVE-2019-8013, CVE-2019-8014, CVE-2019-8015, CVE-2019-8016, CVE-2019-8017, CVE-2019-8018,
CVE-2019-8019, CVE-2019-8020, CVE-2019-8021, CVE-2019-8022, CVE-2019-8023, CVE-2019-8024,
CVE-2019-8025, CVE-2019-8026, CVE-2019-8027, CVE-2019-8028, CVE-2019-8029, CVE-2019-8030,
CVE-2019-8031, CVE-2019-8032, CVE-2019-8033, CVE-2019-8034, CVE-2019-8035, CVE-2019-8036,
CVE-2019-8037, CVE-2019-8038, CVE-2019-8039, CVE-2019-8040, CVE-2019-8041, CVE-2019-8042,
CVE-2019-8043, CVE-2019-8044, CVE-2019-8045, CVE-2019-8046, CVE-2019-8047, CVE-2019-8048,
CVE-2019-8049, CVE-2019-8050, CVE-2019-8051, CVE-2019-8052, CVE-2019-8053, CVE-2019-8054,
CVE-2019-8055, CVE-2019-8056, CVE-2019-8057, CVE-2019-8058, CVE-2019-8059, CVE-2019-8060,
CVE-2019-8061, CVE-2019-8062, CVE-2019-8063, CVE-2019-8077, CVE-2019-8094, CVE-2019-8095,
CVE-2019-8096, CVE-2019-8097, CVE-2019-8098, CVE-2019-8099, CVE-2019-8100, CVE-2019-8101,
CVE-2019-8102, CVE-2019-8103, CVE-2019-8104, CVE-2019-8105, CVE-2019-8106

IOC

-

Zasiahnuté systémy

Adobe After Effects CC 2019 verzie 16 a staršie
Adobe Character Animator CC 2019 verzie 2.1 a staršie
Adobe Premiere Pro CC 2019 verzie 13.1.2 a staršie
Adobe Prelude CC 2019 verzie 8.1 a staršie
Creative Cloud Desktop Application verzie 4.6.1 a staršie
Adobe Acrobat DC, Adobe Acrobat Reader DC
Adobe Experience Manager verzie 6.4, 6.5
Adobe Photoshop CC verzie 19.1.8 a staršie, 20.0.5 a staršie

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

Odporúčania
Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a 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://helpx.adobe.com/security/products/after_effects/apsb19-31.html https://helpx.adobe.com/security/products/character_animator/apsb19-32.html https://helpx.adobe.com/security/products/premiere_pro/apsb19-33.html https://helpx.adobe.com/security/products/prelude/apsb19-35.html https://helpx.adobe.com/security/products/creative-cloud/apsb19-39.html https://helpx.adobe.com/security/products/acrobat/apsb19-41.html https://helpx.adobe.com/security/products/experience-manager/apsb19-42.html https://helpx.adobe.com/security/products/photoshop/apsb19-44.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť v prepínačoch Siemens SCALANCE X

Popis

Spoločnosť Siemens zverejnila informácie o bezpečnostnej zraniteľnosti v prepínačoch produktovej rady SCALANCE X.
Bezpečnostná zraniteľnosť sa nachádza v službe telnet a vzdialený neautentifikovaný útočník by ju prostredníctvom opakovaného zasielania veľkých správ mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

13.08.2019

CVE

CVE-2019-10942

Zasiahnuté systémy

SCALANCE X-200: všetky verzie
SCALANCE X-200IRT: všetky verzie
SCALANCE X-200RNA: všetky verzie

Následky

Zneprístupnenie služby

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame vypnúť službu telnet a na komunikáciu so zariadeniami používať SSH. Rovnako odporúčame zavedením firewallových pravidiel na zariadeniach blokovať port 23/TCP, sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-100232.pdf
https://www.us-cert.gov/ics/advisories/icsa-19-225-03

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

OSIsoft PI Web API Zraniteľnosti

Popis

Spoločnosť OSIsoft LLC zverejnila informácie o bezpečnostných zraniteľnostiach v produkte OSIsoft PI Web API.
Bližšie nešpecifikované zraniteľnosti by neautentifikovaný útočník mohol zneužiť na realizáciu CSRF (Cross-Site Request Forgery) útokov a na získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

13.08.2019

CVE

CVE-2019-13515, CVE-2019-13516

Zasiahnuté systémy

OSIsoft PI Web API 2018 a staršie

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov na verziu PI Web API 2018 SP1 a novšie. Spoločnosť OSIsoft LLC odporúča vypnúť Debug log na Windows zariadeniach, na ktorých beží PI Web API.
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.us-cert.gov/ics/advisories/icsa-19-225-02

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

Identifikátor

Valve Steam game client zraniteľnosť

Popis

Bezpečnostní výskumníci informovali o zraniteľnosti v produkte Steam game client.
Bezpečnostná zraniteľnosť v komponente Steam Client Service umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

07.08.2019

CVE

Zasiahnuté systémy

Steam game client for Windows verzia 5.27.59.20 a staršie

Následky

Eskalácia privilégií

Odporúčania

Spoločnosť Valve Software doposiaľ nevydala aktualizácie odstraňujúce uvedenú zraniteľnosť. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://amonitoring.ru/article/steamclient-0day/
https://gist.github.com/enigma0x3/03f065be011c5980b96855e2741bf302
https://www.bleepingcomputer.com/news/security/steam-zero-day-vulnerability-affects-over-100-million-users/

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

Identifikátor

Intel Zraniteľnosti

Popis

Spoločnosť Intel vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v portfóliu produktov.
Najzávažnejšie zraniteľnosti v produktoch Intel® Processor Identification Utility for Windows a Intel® Computing Improvement Program spočívajú v nedostatočnej implementácii mechanizmov riadenia prístupov v Hardware Abstraction ovládači a lokálny autentifikovaný útočník by ich mohol zneužiť na zneprístupnenie služby, eskaláciu privilégií alebo získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

13.08.2019

CVE

CVE-2019-0173, CVE-2019-11140, CVE-2019-11143, CVE-2019-11145, CVE-2019-11146, CVE-2019-11148, CVE-2019-11162, CVE-2019-11163

Zasiahnuté systémy

Intel(R) RAID Web Console 2 všetky verzie
Intel® NUC Kit NUC7i7DNx, NUC7i5DNx, NUC7i3DNx BIOS verzie 0066 a novšie
Intel® Compute Stick STK2MV64CC BIOS verzie 0060 a novšie
Intel® Compute Card CD1IV128MK BIOS verzie0037 a novšie
Intel® Authenticate verzie staršie ako 3.8
Intel® Driver & Support Assistant verzie staršie ako 19.7.30.2
Intel® Remote Displays SDK verzie staršie ako 2.0.1 R2
Intel® Processor Identification Utility for Windows verzie staršie ako 6.1.0731
Intel® Computing Improvement Program verzie staršie ako 2.4.0.04733.

Následky

Zneprístupnenie služby
Eskalácia privilégií
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00246.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00272.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00275.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00276.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00277.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00281.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00283.html

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

Identifikátor

Kubernetes zraniteľnosti

Popis

Vývojári orchestrátora kontajnerov Kubernetes vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov v API serveri a umožňuje vzdialenému, autentifikovanému útočníkovi vykonávať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

06.08.2019

CVE

CVE-2019-11247, CVE-2019-11249

Zasiahnuté systémy

Kubernetes verzie staršie ako 1.13.9, 1.14.5, and 1.15.2

Následky

Neoprávnený prístup do systému
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.cncf.io/blog/2019/08/06/open-sourcing-the-kubernetes-security-audit/
https://exchange.xforce.ibmcloud.com/vulnerabilities/164767
https://siliconangle.com/2019/08/06/34-vulnerabilities-uncovered-security-audit-kubernetes-code
https://www.theregister.co.uk/2019/08/06/kubernetes_security_audit/
https://seclists.org/oss-sec/2019/q3/117

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

Identifikátor

Delta Industrial Automation DOPSoft Zraniteľnosti

Popis

Spoločnosť Delta Electronics vydala bezpečnostné aktualizácie, ktoré opravujú zraniteľnosti v produkte Delta Industrial Automation DOPSoft.
Bezpečnostné zraniteľnosti by lokálny neautentifikovaný útočník prostredníctvom podvrhnutia špeciálnych Project súborov mohol zneužiť na vykonanie škodlivého kódu, zneprístupnenie služby alebo získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

13.08.2019

CVE

CVE-2019-13513, CVE-2019-13514

Zasiahnuté systémy

DOPSoft Version verzie 4.00.06.15 a staršie

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov a pracovať len s Project súbormi od overených a dôveryhodných 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.us-cert.gov/ics/advisories/icsa-19-225-01

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

Identifikátor

Zraniteľnosti v produktoch Siemens SIPROTEC 5 a DIGSI 5

Popis

Spoločnosť Siemens zverejnila informácie o bezpečnostných zraniteľnostiach v produktoch SIPROTEC 5 a DIGSI 5.
Bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom zasielania špeciálne vytvorených paketov na port 443/TCP mohol zneužiť na zneprístupnenie služby alebo vykonanie neoprávnených zmien v systéme (upload, download alebo odstránenie súborov).

Dátum prvého zverejnenia varovania

13.08.2019

CVE

CVE-2019-10930, CVE-2019-10931

Zasiahnuté systémy

SIPROTEC 5 zariadenia typu 6MD85, 6MD86, 6MD89, 7UM85, 7SA87, 7SD87, 7SL87, 7VK87,7SA82, 7SA86, 7SD82, 7SD86, 7SL82, 7SL86,7SJ86, 7SK82, 7SK85, 7SJ82, 7SJ85, 7UT82,7UT85, 7UT86, 7UT87, 7VE85 s procesormi CP300 a CP100: verzie staršie ako V7.90
SIPROTEC 5 ostatné typy zariadení s procesormi CP300 a CP100: všetky verzie
SIPROTEC 5 relé s procesormi CP200: všetky verzie
Softvér DIGSI 5: verzie staršie ako V7.90

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Spoločnosť Siemens vydala aktualizácie len pre SIPROTEC 5 zariadenia typu 6MD85, 6MD86, 6MD89, 7UM85, 7SA87, 7SD87, 7SL87, 7VK87,7SA82, 7SA86, 7SD82, 7SD86, 7SL82, 7SL86,7SJ86, 7SK82, 7SK85, 7SJ82, 7SJ85, 7UT82,7UT85, 7UT86, 7UT87, 7VE85 a softvér DIGSI 5. Administrátorom odporúčame vykonať aktualizáciu systémov. Rovnako odporúčame zavedením firewallových pravidiel na zariadeniach blokovať prístup k portu 443/TCP a aktivovať RBAC (Role Based Access Control) v zariadeniach s firmvérom verzie V7.80 a vyššie.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-899560.pdf

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

Identifikátor

Zraniteľnosti v produktoch Apache Solr a Apache Spark

Popis

Spoločnosť Apache vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostné zraniteľnosti v produktoch Apache Solr a Spark.
Zraniteľnosť v produkte Apache Spark spočíva v nedostatočnej implementácii kryptografických mechanizmov a vzdialený neautentifikovaný útočník by ju mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom.
Zraniteľnosť v produkte Apache Solr spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v rámci modulu DataImportHandler a vzdialený neautentifikovaný útočník by ju mohol zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

12.08.2019

CVE

CVE-2019-0193, CVE-2019-10099

Zasiahnuté systémy

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

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://tools.cisco.com/security/center/viewAlert.x?alertId=60583
https://tools.cisco.com/security/center/viewAlert.x?alertId=60569

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosti v produktoch Siemens SCALANCE

Popis

Spoločnosť Siemens zverejnila informácie o bezpečnostných zraniteľnostiach v produktoch SCALANCE. Najzávažnejšia zraniteľnosť sa nachádza v produkte SCALANCE SC-60 a lokálny autentifikovaný útočník s fyzickým prístupom k zariadeniu by ju mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.
Druhú zraniteľnosť by vzdialený autentifikovaný útočník mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

13.08.2019

CVE

CVE-2019-10927, CVE-2019-10928

Zasiahnuté systémy

SCALANCE SC-600 verzia 2.0
SCALANCE XB-200 verzia 4.1
SCALANCE XC-200 verzia 4.1
SCALANCE XF-200BA verzia 4.1
SCALANCE XP-200 verzia 4.1
SCALANCE XR-300WG verzia 4.1

Následky

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

Odporúčania

Spoločnosť Siemens zatiaľ vydala bezpečnostnú aktualizáciu len pre zariadenia SCALANCE SC-600. Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Rovnako odporúčame zavedením firewallových pravidiel limitovať prístup k zariadeniam cez port 22/TCP.
Riadiace systémy a jednotky 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://cert-portal.siemens.com/productcert/pdf/ssa-671286.pdf