BEZPEČNOSTNÝ BULLETIN

Týždeň 26. 12. 2018 - 01. 01. 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:
02049/2018/TS/OKB-212

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

Identifikátor

ABB CMS-770 zraniteľnosť

Popis

Spoločnosť ABB informovala o bezpečnostnej zraniteľnosti vo svojom produkte CMS-770.
Bezpečnostná zraniteľnosť je spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

18.12.2018

CVE

CVE-2018-17928

Zasiahnuté systémy

ABB CMS-770 verzia 1.7.1 a staršie

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame uistiť sa, že sú zraniteľné zariadenia nainštalované v súlade s najnovším manuálom spoločnosti ABB dostupnom na nasledujúcom odkaze:
https://library.e.abb.com/public/adcab406985b4510836d4b94490ad953/2CCC481007M0201_User%20Manual.pdf
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje

https://library.e.abb.com/public/6e5e11da5dcf4591a91629356941803f/9ADB005557_ABB_SoftwareVulnerabilityHandlingAdvisory_Rev_D_CMS-770_July_2018.pdf
https://ics-cert.us-cert.gov/advisories/ICSA-18-352-06

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

Identifikátor

Guardzilla IoT Video Camera zraniteľnosť

Popis

Bezpečnostní výskumníci informovali o bezpečnostnej zraniteľnosti v produkte Guardzilla Video Security System GZ521W.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom kryptografickom zabezpečení autentifikačných údajov a umožňuje vzdialenému neautentifikovnaímu útočníkovi získať neoprávnený prístup k citlivým údajom uloženým v Guardzilla cloude na serveroch Amazon Simple Storage Service.

Dátum prvého zverejnenia varovania

27.12.2018

CVE

CVE-2018-5560

Zasiahnuté systémy

Guardzilla All-In-One Video Security System GZ521W

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Spoločnosť Guardzilla doposiaľ nevydala aktualizácie zraniteľného produktu. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://www.0dayallday.org/guardzilla-video-camera-hard-coded-aws-credentials/

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

Identifikátor

Schneider Electric Zelio Soft zraniteľnosť

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoj produkt Zelio Soft, ktorá opravuje bližšie nešpecifikovanú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje lokálnemu neautentifikovanému útočníkovi pomocou podvrhnutia špeciálne upravených Zelio Soft project súborov vykonať škodlivý kód a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.12.2018

CVE

CVE-2018-7817

Zasiahnuté systémy

Schneider Electric Zelio Soft 2 verzie staršie ako v5.2 staršie

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.schneider-electric.com/en/download/document/SEVD-2018-361-01/

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

Identifikátor

Horner Automation Cscape zraniteľnosť

Popis

Spoločnosť Horner Automation vydala bezpečnostnú aktualizáciu na svoj produkt Cscape, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov v Traffic Management Microkernel a umožňuje lokálnemu neautentifikovanému útočníkovi prostredníctvom podvrhnutia upravených POC súborov získať prístup k citlivým údajom a spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

20.12.2018

CVE

CVE-2018-19005

Zasiahnuté systémy

Horner Automation Cscape verzie staršie ako 9.80 SP4

Následky

Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

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-18-354-01

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

Identifikátor

Nagios XI XSS zraniteľnosti

Popis

Spoločnosť Nagios vydala bezpečnostnú aktualizáciu na svoj produkt Nagios XI, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov funkciami magpie_simple.php a magpie_slashbox.php v rss_dashlet/magpierss/scripts/ a umožňujú vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia upravených URL adries vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

20.12.2018

CVE

CVE-2018-20172, CVE-2018-20171

Zasiahnuté systémy

Nagios XI verzie staršie ako 5.5.8

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59340
https://tools.cisco.com/security/center/viewAlert.x?alertId=59341

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

VirusTotal YARA zraniteľnosti

Popis

Spoločnosť VirusTotal vydala bezpečnostnú aktualizáciu na svoj produkt YARA, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti vo funkcii libyara/exec.c spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov umožňujú lokálnemu autentifikovanému útočníkovi získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

21.12.2018

CVE

CVE-2018-19976, CVE-2018-19975, CVE-2018-19974

Zasiahnuté systémy

VirusTotal YARA 3.8.1

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59358
https://tools.cisco.com/security/center/viewAlert.x?alertId=59359
https://tools.cisco.com/security/center/viewAlert.x?alertId=59360

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.3
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

BIG-IP ARM BGP zraniteľnosť

Popis

Spoločnosť F5 vydala bezpečnostnú aktualizáciu na svoj produkt BIG-IP (LTM), ktorá opravuje bezpečnostnú zraniteľnosť v komponente BGP daemon (bgpd).
Bezpečnostná zraniteľnosť umožňuje vzdialenému útočníkovi prostredníctvom podvrhnutia upravených identifikátorov autonómnych systémov (ASN) spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

27.12.2018

CVE

CVE-2018-17539

Zasiahnuté systémy

BIG-IP (LTM) verzie staršie ako 14.1.0/14.0.0.3; 13.1.1.2; 12.1.3.7 a 11.6.3.3

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.f5.com/csp/article/K17264695