BEZPEČNOSTNÝ BULLETIN

Týždeň 05. 12. 2018 - 11. 12. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

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

Identifikátor

MISP zraniteľnosť

Popis

Vývojári platformy MISP vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť vo funkcii app/Model/Event.php.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov zasiahnutým systémom a umožňuje vzdialenému autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov spôsobiť vykonanie škodlivých príkazov.

Dátum prvého zverejnenia varovania

06.12.2018

CVE

CVE-2018-19908

Zasiahnuté systémy

MISP verzie staršie ako 2.4.99

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.misp-project.org/2018/12/06/MISP.2.4.99.released.html
https://github.com/MISP/MISP/releases/tag/v2.4.99
https://nvd.nist.gov/vuln/detail/CVE-2018-19908

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

Identifikátor

Viacero zraniteľností v PHP

Popis

Vývojári skriptovacieho jazyka PHP vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero chýb a bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.12.2018

CVE

-

Zasiahnuté systémy

PHP 7.2 verzie staršie ako 7.2.13
PHP 7.1 verzie staršie ako 7.1.25
PHP 7.0 verzie staršie ako 7.0.33
PHP 5.6 verzie staršie ako 5.6.39

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-php-could-allow-for-arbitrary-code-execution_2018-136/

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

Identifikátor

Rockwell Automation MicroLogix ControlLogix zraniteľnosť

Popis

Spoločnosť Rockwell Automation vydala bezpečnostné aktualizácie na svoje PLC produkty MicroLogix 1400 a 1756 ControlLogix, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom zasielania CIP požiadaviek vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

06.12.2018

CVE

CVE-2018-17924

Zasiahnuté systémy

Rockwell Automation MicroLogix 1400 Controllers
Rockwell Automation 1756 ControlLogix EtherNet/IP Communications Modules

Následky

Zneprístupnenie služby, Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu. Odporúčame tiež na zasiahnutých zariadeniach blokovať prístup na porty 44818 a 2222 TCP a UDP.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-310-02

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

Identifikátor

ZTE ZXIN10 zraniteľnosť

Popis

Spoločnosť ZTE vydala bezpečnostnú aktualizáciu na svoj produkt ZXIN10-Orange, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov v devcomm procese a umožňuje vzdialenému neautentifikovanému útočníkovi vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

07.12.2018

CVE

CVE-2018-7364

Zasiahnuté systémy

ZXIN10-Orange verzie staršie ako ZXINOS-RESV1.01.44

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1009943
https://exchange.xforce.ibmcloud.com/vulnerabilities/154049

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

Identifikátor

GE Proficy GDS zraniteľnosť

Popis

Spoločnosť General Electric vydala bezpečnostnú aktualizáciu na svoj produkt Proficy GDS, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených XML súborov získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

06.12.2018

CVE

CVE-2018-15362

Zasiahnuté systémy

General Electric Proficy GDS verzie staršie ako 2.1 (Cimplicity 9.0 R2, Cimplicity 9.5, Cimplicity 10.0)

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-340-01

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

Identifikátor

Eurotherm by Schneider Electric GUIcon zraniteľnosti

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoj produkt Eurotherm GUIcon, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú lokálnemu neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených GD1 súborov vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

04.12.2018

CVE

CVE-2018-7813, CVE-2018-7814, CVE-2018-7815

Zasiahnuté systémy

Eurotherm by Schneider Electric GUIcon verzie staršie ako 2.0 (Gold Build 683.003)

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.

Zdroje

https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2018-338-01-Eurotherm-GUIcon.pdf&p_Doc_Ref=SEVD-2018-338-01

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

Identifikátor

McAfee True Key zraniteľnosti

Popis

Spoločnosť McAfee vydala bezpečnostnú aktualizáciu na svoj produkt True Key, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú lokálnemu autentifikovanému útočníkovi vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

06.12.2018

CVE

CVE-2018-6755, CVE-2018-6756, CVE-2018-6757

Zasiahnuté systémy

McAfee True Key Windows Client verzie staršie ako 5.2.167.1

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://service.mcafee.com/FAQDocument.aspx?&id=TS102872

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.0**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Linux PolicyKit zraniteľnosť

Popis

Bezpečnostní výskumníci vydali upozornenie na bezpečnostnú zraniteľnosť v Policykit komponente unixových operačných systémov.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov pri spracúvaní UID väčších ako 2147483647 a umožňuje lokálnemu autentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

02.12.2018

CVE

CVE-2018-19788

Zasiahnuté systémy

PolicyKit 0.115 (unixové operačné systémy Red Hat, Debian, Ubuntu, CentOS, SUSE a ďalšie)

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame v konfiguračných súboroch adduser.conf a login.defs zakázať vytváranie UID s negatívnymi hodnotami a tiež hodnotami väčšími ako 2147483646.

Zdroje

http://www.linuxsecurity.com/content/view/215180?rdf
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=915332
https://nvd.nist.gov/vuln/detail/CVE-2018-19788
https://thehackernews.com/2018/12/linux-user-privilege-policykit.html
https://access.redhat.com/security/cve/cve-2018-19788

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Norton Password Manager for Android XSS zraniteľnosť

Popis

Spoločnosť Symantec vydala bezpečnostnú aktualizáciu na svoj produkt Norton Password Manager for Android, ktorá opravuje XSS bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje autentifikovanému útočníkovi s fyzickým prístupom k zariadeniu vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

06.12.2018

CVE

CVE-2018-18362

Zasiahnuté systémy

Norton Password Manager for Android verzie staršie ako 6.1.0.1045

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.symantec.com/en_US/article.SYMSA1470.html