BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 06. 2018 – 12. 06. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	VMware AirWatch Agent Vulnerability	Vysoká	**8.9**
02.	Google Chrome Stable Channel Update	Vysoká	**8.8**
03.	Mozilla Foundation Firefox Security Advisory 2018-14	Vysoká	**8.8**
04.	Rockwell Automation RSLinx Classic and FactoryTalk Linx Gateway Vulnerability	Vysoká	**8.8**
05.	Philips IntelliVue Patient and Avalon Fetal Monitors Multiple Vulnerabilities	Vysoká	**8.3**
06.	IBM Robotic Process Automation Vulnerabilities	Vysoká	**8.0**
07.	Ubuntu LTS Has Multiple Elfutils Vulnerabilities	Vysoká	**7.8**
08.	Foscam Cameras Multiple Vulnerabilities	Vysoká	**7.5**
09.	Trend Micro OfficeScan Multiple Vulnerabilities	Stredná	**6.1**
10.	GnuPG mainproc.c spoofing	Stredná	**5.3**

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-072

BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 06. 2018 – 12. 06. 2018

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.9**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

VMware AirWatch Agent Vulnerability

Popis

Spoločnosť VMWare vydala bezpečnostnú aktualizáciu na svoj produkt AirWatch Agent, ktorá opravuje bezpečnostnú zraniteľnosť vo File Manager komponente.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných opatrení a umožňuje vzdialenému útočníkovi vykonať škodlivý kód a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.06.2018

CVE

CVE-2018-6968

Zasiahnuté systémy

VMware AirWatch Agent for Android verzie staršie ako 8.2
VMware AirWatch Agent for Windows Mobile verzie staršie ako 6.5.2

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2018-0015.html
https://support.workspaceone.com/articles/360005681594

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-072

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

Identifikátor

Google Chrome Stable Channel Update

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu, ktorá rieši viacero chýb a bezpečnostnú zraniteľnosť v internetovom prehliadači Chrome.
Bližšie nešpecifikovanú bezpečnostnú zraniteľnosť, ktorá spočíva v nesprávnom spracovávaní CSP (Content Security Policy) hlavičiek by vzdialený neautentifikovaný útočník mohol zneužiť na reazlizáciu XSS (Cross-Site Scripting) útokov a následné vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

06.06.2018

CVE

CVE-2018-6148

Zasiahnuté systémy

Google Chrome verzie staršie ako 67.0.3396.79

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://chromereleases.googleblog.com/search/label/Stable%20updates
https://thehackernews.com/2018/06/google-chrome-csp.html

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

Identifikátor

Mozilla Foundation Firefox Security Advisory 2018-14

Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu, ktorá rieši bezpečnostnú zraniteľnosť v prehliadači Firefox.
Bezpečnostná zraniteľnosť sa nachádza v knižnici Skia a vzdialený neautentifikovaný útočník by ju mohol zneužiť prostredníctvom podvrhnutia špeciálne vytvorených SVG súborov na vykonanie škodlivého kódu v kontexte webového prehliadača a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.06.2018

CVE

CVE-2018-6126

Zasiahnuté systémy

Mozilla Firefox verzie staršie ako 60.0.2, ESR 60.0.2, a ESR 52.8.1

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2018-14/

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

Identifikátor

Rockwell Automation RSLinx Classic and FactoryTalk Linx Gateway Vulnerability

Popis

Spoločnosť Rockwell Automation vydala bezpečnostné aktualizácie, ktoré odstraňujú bezpečnostnú zraniteľnosť v produktoch RSLinx Classic a FactoryTalk Linx Gateway.
Bezpečnostná zraniteľnosť spočíva v nesprávnom spracovaní adries, ktoré v sebe obsahujú medzeru a vzdialený autentifikovaný útočník by ju mohol zneužiť na vykonanie škodlivého kódu a eskaláciu privilégií.

Dátum prvého zverejnenia varovania

07.06.2018

CVE

CVE-2018-10619

Zasiahnuté systémy

RSLinx Classic verzie 3.90.01 a staršie
FactoryTalk Linx Gateway verzie 3.90.00 a staršie

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-158-01

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

Identifikátor

Philips IntelliVue Patient and Avalon Fetal Monitors Multiple Vulnerabilities

Popis

Spoločnosť Philips vydala upozornenie na trojicu bližšie nešpecifikovaných bezpečnostných zraniteľností v zdravotníckych produktoch IntelliVue Patient Monitor a Avalon Fetal Monitor. Uvedené zraniteľnosti je možné zneužiť, len ak sa útočník nachádza v rovnakej podsieti ako zasiahnuté zariadenia.
Prvú zraniteľnosť by neautentifikovaný útočník mohol zneužiť na modifikáciu obsahu pamäti zariadení.
Druhú zraniteľnosť by neautentifikovaný útočník mohol zneužiť na neoprávnený prístup k údajom v pamäti zariadení.
Poslednú zraniteľnosť by neautentifikovaný útočník mohol zneužiť na prístup a modifikáciu obsahu pamäti alebo zneprístupnenie služby na zariadení.

Dátum prvého zverejnenia varovania

05.06.2018

CVE

CVE-2018-10597, CVE-2018-10599, CVE-2018-10601

Zasiahnuté systémy

IntelliVue Patient Monitors série MP (MP2/X2/MP30/MP50/MP70/NP90/MX700/800) Rev B-M
IntelliVue Patient Monitors série MX (MX400-550) Rev J-M a (X3/MX100) Rev M
Avalon Fetal/Maternal Monitors FM20/FM30/FM40/FM50 Rev F.0, G.0 a J.3

Následky

Neoprávnená zmena v systéme, Zneprístupnenie služby

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov. Administrátorom tiež odporúčame limitovať prístup k zasiahnutým zariadeniam a ich funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://www.usa.philips.com/healthcare/about/customer-support/product-security
https://ics-cert.us-cert.gov/advisories/ICSMA-18-156-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

IBM Robotic Process Automation Vulnerabilities

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Robotic Process Automation, ktorá opravuje viacero bezpečnostných zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nekorektných operáciách pri spracovaní CSV súborov a umožňuje vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného CSV súboru vykonať škodlivý kód na napadnutom systéme.

Dátum prvého zverejnenia varovania

30.05.2018

CVE

CVE-2018-1547, CVE-2018-1514

Zasiahnuté systémy

IBM Robotic Process Automation with Automation Anywhere V10.0.0.0

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://www-01.ibm.com/support/docview.wss?uid=swg22016197
http://www-01.ibm.com/support/docview.wss?uid=swg22016099

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

Identifikátor

Ubuntu LTS Has Multiple Elfutils Vulnerabilities

Popis

Vývojári operačného systému Ubuntu vydali bezpečnostnú aktualizáciu, ktorá opravuje viaceré zraniteľnosti v balíku elfutils.
Zraniteľnosti spočívajú v nesprávnom spracovaní ELF (Executable and Linkable Format) súborov v rámci libebl/ebldynamictagname.c, elfint.c (funkcie check_symtab_shndx, check_sysv_hash), elf_getdata.c (funkcia__libelf_set_rawdata_wrlock), readelf.c (funkcia handle_gnu_hash), eblobjnotetypename.c (funkcia ebl_object_note_type_name), common. (funkcia allocate_elf) a v elf_compress.c.
Uvedené zraniteľnosti by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne vytvorených ELF súborov zneužiť na vykonanie škodlivého kódu a zneprístupnenie služby.
Na uvedené zraniteľnosti sú voľne dostupné exploity.

Dátum prvého zverejnenia varovania

05.06.2018 (posledná aktualizácia 07.06.2018)

CVE

CVE-2017-7607, CVE-2017-7608, CVE-2017-7609, CVE-2017-7610, CVE-2017-7611, CVE-2017-7612, CVE-2017-7613, CVE-2016-10254, CVE-2016-10255

Zasiahnuté systémy

Ubuntu 16.04 LTS
Ubuntu 14.04 LTS

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby

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.

Zdroje

https://usn.ubuntu.com/3670-1/
https://www.auscert.org.au/bulletins/63622
https://sourceware.org/bugzilla/show_bug.cgi?id=22976
https://nvd.nist.gov/vuln/detail/CVE-2018-8769

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

Identifikátor

Foscam Cameras Multiple Vulnerabilities

Popis

Spoločnosť Foscam vydala bezpečnostné aktualizácie na svoje IP bezpečnostné kamery, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných opatrení vo webService komponente a umožňujú vzdialenému neautentifikovanému útočníkovi obísť autentifikačné mechanizmy a eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

06.06.2018

CVE

CVE-2018-6830, CVE-2018-6831, CVE-2018-6832

Zasiahnuté systémy

C1 Lite V3, C1 V3, FI9800P V3, FI9803P V4, FI9816P V3, FI9821EP V2, FI9821P V3, FI9826P V3, FI9831P V3, FI9851P V3, FI9853EP V2, C1, C1 V2, C1 Lite, C1 Lite V2, FI9800P, FI9800P V2, FI9803P V2, FI9803P V3, FI9815P, FI9815P V2, FI9816P, FI9816P V2, FI9851P V2, R2, C2, R4, FI9900EP, FI9900P, FI9901EP, FI9961EP, FI9928P, FI9803EP, FI9803P, FI9853EP, FI9851P, FI9821P V2, FI9826P V2, FI9831P V2, FI9821EP, FI9821W V2, FI9818W V2, FI9831W, FI9826W, FI9821P, FI9831P, FI9826P, FI9805W, FI9804W, FI9804P, FI9805E, FI9805P, FI9828P, FI9828W, FI9828P V2

Následky

Eskalácia privilégií, Zneprístupnenie služby, Neoprávnený prístup do systému, Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://blog.vdoo.com/2018/06/06/vdoo-has-found-major-vulnerabilities-in-foscam-cameras/
https://www.bleepingcomputer.com/news/security/patches-available-for-dangerous-bugs-in-popular-brand-of-ip-cameras/

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

Identifikátor

Trend Micro OfficeScan Multiple Vulnerabilities

Popis

Spoločnosť Trend Micro vydala bezpečnostnú aktualizáciu na svoj produkt OfficeScan, ktorá opravuje viacero bezpečnostných zraniteľností.
Najvážnejšie bezpečnostné zraniteľnosti v ovládači TMWFP spočívajú v nesprávnom overovaní používateľských vstupov a umožňujú lokálnemu autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených dát eskalovať svoje privilégiá na napadnutom systéme a získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

06.06.2018 (aktualizované 08.06.2018)

CVE

CVE-2018-10358, CVE-2018-10359, CVE-2018-10505, CVE-2018-10506, CVE-2018-10507, CVE-2018-10508, CVE-2018-10509

Zasiahnuté systémy

OfficeScan XG, OfficeScan XG SP1, OfficeScan 11.0 SP1

Následky

Eskalácia privilégií, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://success.trendmicro.com/solution/1119961

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

Identifikátor

GnuPG mainproc.c spoofing

Popis

Vývojári šifrovacieho programu GnuPG vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v mainproc.c komponente.
Protokol OpenPGP umožňuje do podpísanej alebo šifrovanej správy zahrnúť aj názov priloženého súboru. Počas dešifrovania a overovania obsahu správy ho GPG nástroj môže zobrazovať na konzole. Pred zobrazením však nedochádza k overovaniu zobrazeného reťazca na prítomnosť riadiacich a špeciálnych znakov. Túto zraniteľnosť by útočník mohol prostredníctvom špeciálne vytvoreného názvu súboru zneužiť na podvrhnutie stavových správ PGP, ktoré ostatné programy využívajú na získanie informácií o správnosti podpisu a ostatných parametrov.

Dátum prvého zverejnenia varovania

08.06.2018

CVE

CVE-2018-12020

Zasiahnuté systémy

GnuPG verzie staršie ako 2.2.8

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://lists.gnupg.org/pipermail/gnupg-announce/2018q2/000425.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/144556