BEZPEČNOSTNÝ BULLETIN

Týždeň 19. 12. 2018 - 25. 12. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	ASUS Aura Sync zraniteľnosti	Vysoká	**8.4**
02.	GIGABYTE Drivers zraniteľnosti	Vysoká	**8.4**
03.	IBM Trusteer Rapport zraniteľnosť	Vysoká	**8.3**
04.	FactoryTalk Services Platform zraniteľnosť	Vysoká	**7.5**
05.	GNU Wget zraniteľnosť	Stredná	**6.2**
06.	ChinaMobile PLC Wireless Router zraniteľnosť	Stredná	**6.1**

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-211

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

Identifikátor

ASUS Aura Sync zraniteľnosti

Popis

Bezpečnostní výskumníci informovali o bezpečnostných zraniteľnostiach v produkte ASUS Aura Sync. Najzávažnejšie bezpečnostné zraniteľnosti v ovládačoch GLCKIo a Asusgio umožňujú lokálnemu neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.12.2018

CVE

CVE-2018-18537, CVE-2018-18536, CVE-2018-18535

Zasiahnuté systémy

ASUS Aura Sync verzia 1.07.22 a staršie

Následky

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

Odporúčania

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

Zdroje

https://www.secureauth.com/labs/advisories/asus-drivers-elevation-privilege-vulnerabilities
https://exchange.xforce.ibmcloud.com/vulnerabilities/154735
https://exchange.xforce.ibmcloud.com/vulnerabilities/154736

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

Identifikátor

GIGABYTE Drivers zraniteľnosti

Popis

Bezpečnostní výskumníci informovali o bezpečnostných zraniteľnostiach v ovládačoch spoločnosti Gigabyte.
Najzávažnejšie bezpečnostné zraniteľnosti v ovládačoch GPCIDrv a GDrv umožňujú lokálnemu neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.12.2018

CVE

CVE-2018-19320, CVE-2018-19322, CVE-2018-19323, CVE-2018-19321

Zasiahnuté systémy

GIGABYTE APP Center v1.05.21 a staršie
AORUS GRAPHICS ENGINE v1.33 a staršie
XTREME GAMING ENGINE v1.25 a staršie
OC GURU II v2.08

Následky

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

Odporúčania

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

Zdroje

https://www.secureauth.com/labs/advisories/gigabyte-drivers-elevation-privilege-vulnerabilities

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

Identifikátor

IBM Trusteer Rapport zraniteľnosť

Popis

Bezpečnostní výskumníci informovali o bezpečnostnej zraniteľnosti v produkte IBM Trusteer Rapport. Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.12.2018

CVE

-

Zasiahnuté systémy

IBM Trusteer Rapport 3.6.1908 pre MacOS

Následky

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

Odporúčania

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

Zdroje

https://www.trustwave.com/en-us/resources/security-resources/security-advisories/?fid=21465
https://www.cybersecurity-help.cz/vdb/SB2018122507
https://securityaffairs.co/wordpress/79141/hacking/kernel-buffer-overflow-trusteer-rapport.html

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

Identifikátor

FactoryTalk Services Platform zraniteľnosť

Popis

Bezpečnostní výskumníci informovali o bezpečnostnej zraniteľnosti v produkte FactoryTalk Services Platform.
Bezpečnostná zraniteľnosť umožňuje vzdialenému neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.12.2018

CVE

CVE-2018-18981

Zasiahnuté systémy

Rockwell Automation FactoryTalk Services Platform staršie ako verzia 3.00

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-331-02

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

Identifikátor

GNU Wget zraniteľnosť

Popis

Vývojári linuxového nástroja GNU Wget vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť vo funkcii set_file_metadata v xattr.c .
Bezpečnostná zraniteľnosť spočíva v nesprávnom spracovaní ukladaných metadát a umožňuje lokálnemu útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

25.12.2018

CVE

CVE-2018-20483

Zasiahnuté systémy

GNU Wget verzie staršie ako 1.20.1

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2018-20483
https://www.suse.com/security/cve/CVE-2018-20483/
https://securityaffairs.co/wordpress/79413/security/wget-flaw.html

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

Identifikátor

ChinaMobile PLC Wireless Router zraniteľnosť

Popis

Bezpečnostní výskumníci informovali o bezpečnostnej zraniteľnosti v produkte PLC Wireless Router GPN2.4P21-C-CN.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom XSS útoku získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

21.12.2018

CVE

CVE-2018-20326

Zasiahnuté systémy

ChinaMobile PLC Wireless Router GPN2.4P21-C-CN (Firmware: W2001EN-00)

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

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

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/154852
https://packetstormsecurity.com/files/150918