BEZPEČNOSTNÝ BULLETIN

Týždeň 05. 06. 2019 - 11. 06. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome viacero zraniteľností	Vysoká	**8.8**
02.	Zraniteľnosti riadiacich jednotiek ABB	Vysoká	**8.8**
03.	Phoenix Contact FL NAT SMx Ethernet Switch zraniteľnosť	Vysoká	**8.8**
04.	Cisco Unified Communications Manager IM&P Service, Cisco TelePresence VCS a Cisco Expressway Series zraniteľnosť	Vysoká	**8.6**
05.	Phoenix Contact PLCNext AXC F 2152 zraniteľnosti	Vysoká	**7.6**
06.	VLC viacero zraniteľností	Vysoká	**7.5**
07.	Dameware Remote Mini Control zraniteľnosti	Vysoká	**7.4**
08.	Panasonic Control FPWIN Pro zraniteľnosti	Vysoká	**7.3**
09.	Cisco Industrial Network Director zraniteľnosť	Vysoká	**7.2**
10.	Geutebrück G-Cam a G-Code zraniteľnosti	Vysoká	**7.2**
11.	Yubico pam-u2f	Stredná	**6.2**

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-156

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 z týchto zraniteľností sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a 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

04.06.2019

CVE

CVE-2019-5828, CVE-2019-5829, CVE-2019-5830, CVE-2019-5831, CVE-2019-5832, CVE-2019-5833, CVE-2019-5834, CVE-2019-5835, CVE-2019-5836, CVE-2019-5837, CVE-2019-5838, CVE-2019-5839, CVE-2019-5840

Zasiahnuté systémy

Google Chrome verzie staršie ako 75.0.3770.80

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/2019/06/stable-channel-update-for-desktop.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2019-060/

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

Identifikátor

Zraniteľnosti riadiacich jednotiek ABB

Popis

Spoločnosť ABB vydala bezpečnostné aktualizácie na viacero svojich riadiacich jednotiek. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v existencii zabudovaného administrátorského účtu s predvoleným heslom a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnenú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

05.06.2019

CVE

CVE-2019-7225, CVE-2019-7226, CVE-2019-7227, CVE-2019-7228, CVE-2019-7229, CVE-2019-7230, CVE-2019-7232

Zasiahnuté systémy

CP620, order code: 1SAP520100R0001, revision index G1 with BSP UN31 V1.76 a staršie
CP620, order code: 1SAP520100R4001, revision index G1 with BSP UN31 V1.76 a staršie
CP620-WEB, order code: 1SAP520200R0001, revision index G1 with BSP UN31 V1.76 a staršie
CP630, order code: 1SAP530100R0001, revision index G1 with BSP UN31 V1.76 a staršie
CP630-WEB, order code: 1SAP530200R0001, revision index G1 with BSP UN31 V1.76 a staršie
CP635, order code: 1SAP535100R0001, revision index G1 with BSP UN31 V1.76 a staršie
CP635, order code: 1SAP535100R5001, revision index G1 with BSP UN31 V1.76 a staršie
CP635-B, order code: 1SAP535100R2001, revision index G1 with BSP UN31 V1.76 a staršie
CP635-WEB, order code: 1SAP535200R0001, revision index G1 with BSP UN31 V1.76 a staršie
CP651, order code: 1SAP551100R0001, revision index B1 with BSP UN30 V1.76 a staršie
CP651-WEB, order code: 1SAP551200R0001, revision index A0 with BSP UN30 V1.76 a staršie
CP661, order code: 1SAP561100R0001, revision index B1 with BSP UN30 V1.76 a staršie
CP661-WEB, order code: 1SAP561200R0001, revision index A0 with BSP UN30 V1.76 a staršie
CP665, order code: 1SAP565100R0001, revision index B1 with BSP UN30 V1.76 a staršie
CP665-WEB, order code: 1SAP565200R0001, revision index A0 with BSP UN30 V1.76 a staršie
CP676, order code: 1SAP576100R0001, revision index B1 with BSP UN30 V1.76 a staršie
CP676-WEB, order code: 1SAP576200R0001, revision index A0 with BSP UN30 V1.76 a staršie
PB610 Panel Builder 600, order code: 1SAP500900R0101, verzie 1.91 až 2.8.0.367

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup do systému

Odporúčania
Administrátorom odporúčame bezodkladne 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. Ďalej odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL). Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje
https://search.abb.com/library/Download.aspx?DocumentID=3ADR010402&LanguageCode=en&DocumentPartId=&Action=Launch https://search.abb.com/library/Download.aspx?DocumentID=3ADR010377&LanguageCode=en&DocumentPartId=&Action=Launch https://search.abb.com/library/Download.aspx?DocumentID=3ADR010376&LanguageCode=en&DocumentPartId=&Action=Launch

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

Identifikátor

Phoenix Contact FL NAT SMx Ethernet Switch zraniteľnosť

Popis

Spoločnosť Phoenix Contact zverejnila informácie o bezpečnostnej zraniteľnosti vo svojom produkte FL NAT SMx Ethernet Switch.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

04.06.2019

CVE

CVE-2019-9744

Zasiahnuté systémy

PHOENIX CONTACT FL NAT SMN 8TX-M (2702443)
PHOENIX CONTACT FL NAT SMN 8TX-M-DMG (2989352)
PHOENIX CONTACT FL NAT SMN 8TX (2989365)
PHOENIX CONTACT FL NAT SMCS 8TX (2989378)

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať deaktiváciu webového rozhrania (WEB-UI) a vykonávať konfigurácie systému prostredníctvom SNMP protokolu.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-155-02

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

Identifikátor

Cisco Unified Communications Manager IM&P Service, Cisco TelePresence VCS a Cisco Expressway Series zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje produkty Unified Communications Manager IM&P, Cisco TelePresence VCS a Cisco Expressway Series, ktoré opravujú bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

05.06.2019

CVE

CVE-2019-1845

Zasiahnuté systémy

Expressway Series configured for Mobile and Remote Access with IM&P Service verzie od X8.1 do X12.5.2
elePresence VCS configured for Mobile and Remote Access with IM&P Service verzie od X8.1 do X12.5.2
Unified Communications Manager IM&P Service viacero verzií

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190605-cucm-imp-dos

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Phoenix Contact PLCNext AXC F 2152 zraniteľnosti

Popis

Spoločnosť Phoenix Contact zverejnila informácie o bezpečnostných zraniteľnostiach vo viacerých komponentoch svojho produktu AXC F 2152 firmware. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

04.06.2019

CVE

CVE-2015-9251, CVE-2016-1247, CVE-2016-6301, CVE-2016-7103, CVE-2016-7141, CVE-2016-7444, CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843, CVE-2016-9952, CVE-2016-9953, CVE-2017-1000100, CVE-2017-1000101, CVE-2017-1000254, CVE-2017-1000257, CVE-2017-11108, CVE-2017-11185, CVE-2017-11541, CVE-2017-11542, CVE-2017-11543, CVE-2017-15906, CVE-2017-3731, CVE-2017-3735, CVE-2017-3737, CVE-2017-3738, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2017-8816, CVE-2017-8817, CVE-2017-9022, CVE-2017-9023, CVE-2017-9233, CVE-2018-0737, CVE-2018-1000005, CVE-2018-1000117, CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122, CVE-2018-1000301, CVE-2018-5388, CVE-2018-7559, CVE-2019-10997, CVE-2019-10998

Zasiahnuté systémy

PHOENIX CONTACT AXC F 2152 s firmware verziou 1

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-155-01

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

Identifikátor

VLC viacero zraniteľností

Popis

Vývojári multimediálneho prehrávača VLC vydali aktualizáciu svojho produktu, ktorá rieši viacero chýb a 43 bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služieb a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

07.06.2019

CVE

-

Zasiahnuté systémy

VLC Media Player verzie staršie ako 3.0.7

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.bleepingcomputer.com/news/software/vlc-307-is-biggest-security-release-due-to-eu-bounty-program/
https://gbhackers.com/vlc-3-0-7-released/amp/
https://www.videolan.org/developers/vlc-branch/NEWS

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.4
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Dameware Remote Mini Control zraniteľnosti

Popis

Spoločnosť Dameware vydala bezpečnostnú aktualizáciu na svoj produkt Remote Mini Control, ktorá rieši viacero bezpečnostných zraniteľností. Najvážnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

07.06.2019

CVE

CVE-2019-3955, CVE-2019-3956, CVE-2019-3957

Zasiahnuté systémy

Dameware Remote Mini Control verzie staršie ako 12.1.2.00

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.tenable.com/security/research/tra-2019-26
https://www.tenable.com/cve/CVE-2019-3955
https://www.tenable.com/cve/CVE-2019-3956
https://www.tenable.com/cve/CVE-2019-3957
https://support.solarwinds.com/SuccessCenter/s/article/Dameware-Mini-Remote-Control-12-1-0-Hotfix-2-Release-Notes

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.3**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Panasonic Control FPWIN Pro zraniteľnosti

Popis

Spoločnosť Panasonic vydala bezpečnostné aktualizácie na svoj produkt Vijeo Citect, ktoré opravujú bezpečnostné zraniteľnosti. Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú lokálnemu, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.06.2019

CVE

CVE-2019-6530, CVE-2019-6532

Zasiahnuté systémy

Panasonic FPWIN Pro verzie staršie ako 7.3.1.0

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne 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://ics-cert.us-cert.gov/advisories/ICSA-19-157-02
https://www.panasonic-electric-works.com/eu/plc-software-control-fpwin-pro.htm

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

Identifikátor

Cisco Industrial Network Director zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoj produkt Cisco Industrial Network Director, ktoré opravujú bezpečnostné zraniteľnosti. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.06.2019

CVE

CVE-2019-1861

Zasiahnuté systémy

Cisco Industrial Network Director verzie staršie ako 1.6.0.

Následky

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

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/content/CiscoSecurityAdvisory/cisco-sa-20190605-ind-rce#vp

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

Identifikátor

Geutebrück G-Cam a G-Code zraniteľnosti

Popis

Spoločnosť Geuterbrück vydala bezpečnostné aktualizácie na svoje produkty G-Cam a G-Code, ktoré opravujú bezpečnostné zraniteľnosti. Najzávažnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému, autentifikovanému útočníkovi s administrátorským prístupom vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.06.2019

CVE

CVE-2019-10956, CVE-2019-10957, CVE-2019-10958

Zasiahnuté systémy

Geutebrück G-Code verzie staršie ako 1.12.13.2
Geutebrück G-Cam verzie staršie ako 1.12.13.2

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-155-03
https://portal.geutebrueck.com/

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

Identifikátor

Yubico pam-u2f

Popis

Vývojári Yubico pam-u2f zverejnili informácie o bezpečnostnej zraniteľnosti modulu pam-u2f. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

05.06.2019

CVE

CVE-2019-12209

Zasiahnuté systémy

Yubico pam-u2f verzie staršie ako 1.0.8

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/162187
https://seclists.org/oss-sec/2019/q2/149
https://github.com/Yubico/pam-u2f/commit/7db3386fcdb454e33a3ea30dcfb8e8960d4c3aa3