BEZPEČNOSTNÝ BULLETIN

Týždeň 04. 08. 2021 - 10. 08. 2021

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:
01439/2020/SK-CERT-510

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

Identifikátor

mySCADA myPRO - viacero bezpečnostných zraniteľností

Popis

Spoločnosť mySCADA vydala bezpečnostnú aktualizáciu na produkt myPRO, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

06.08.2021

CVE

CVE-2021-27505, CVE-2021-33005, CVE-2021-33009, CVE-2021-33013

Zasiahnuté systémy

myPRO vo verzii staršej ako 8.20.0

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom 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://us-cert.cisa.gov/ics/advisories/icsa-21-217-03

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

Identifikátor

FATEK Automation FvDesigner produkt - viacero bezpečnostných zraniteľností

Popis

Spoločnosť FATEK Automation vydala bezpečnostnú aktualizáciu na produkt FvDesigner, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.08.2021

CVE

CVE-2021-32931, CVE-2021-32939, CVE-2021-32947

Zasiahnuté systémy

FvDesigner vo verzii staršej ako 1.5.88 (vrátane)

Následky

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

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Administrátorom 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://us-cert.cisa.gov/ics/advisories/icsa-21-217-02

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.7**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Phoenix Contact PLCnext Control produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Phoenix Contact vydala bezpečnostnú aktualizáciu na svoje portfólio produktov PLCnext Control, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej JSON požiadavky, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

04.08.2021

CVE

CVE-2021-34570

Zasiahnuté systémy

AXC F 1152 vo verzii staršej ako 2021.0.5 LTS
AXC F 2152 vo verzii staršej ako 2021.0.5 LTS
AXC F 3152 vo verzii staršej ako 2021.0.5 LTS
RFC 4072S vo verzii staršej ako 2021.0.5 LTS
AXC F 2152 Starterkit vo verzii staršej ako 2021.0.5 LTS
PLCnext Technology Starterkit vo verzii staršej ako 2021.0.5 LTS

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

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

Zdroje

https://cert.vde.com/en-us/advisories/vde-2021-029

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

Identifikátor

Bosch IP kamery - bezpečnostná zraniteľnosť

Popis

Spoločnosť Bosch vydala bezpečnostné aktualizácie na svoje portfólio IP kamier, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.08.2021

CVE

CVE-2021-23849

Zasiahnuté systémy

CPP4 s firmware vo verzii staršej ako 7.10 (vrátane)
CPP6 s firmware vo verzii staršej ako 7.61 (vrátane)
CPP6 s firmware vo verzii staršej ako 7.81.0060
AVIOTEC s firmware vo verzii staršej ako 7.81.0060
CPP7 s firmware vo verzii staršej ako 7.61 (vrátane)
CPP7 s firmware vo verzii staršej ako 7.81.0060
CPP7.3 s firmware vo verzii staršej ako 7.62 (vrátane)
CPP7.3 s firmware vo verzii staršej ako 7.81.0060
CPP13 s firmware vo verzii staršej ako 7.75 (vrátane)
CPP14 s firmware vo verzii staršej ako 8.00 (vrátane)

Následky

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

Odporúčania

Administrátorom a používateľom 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://psirt.bosch.com/security-advisories/bosch-sa-033305-bt.html

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

Identifikátor

Rust - bezpečnostná zraniteľnosť

Popis

Vývojári programovacieho jazyka Rust vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

08.08.2021

CVE

CVE-2021-29922

Zasiahnuté systémy

Rust vo verzii staršej ako 1.53.0

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://github.com/sickcodes/security/blob/master/advisories/SICK-2021-015.md
https://www.rust-lang.org/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29922
https://exchange.xforce.ibmcloud.com/vulnerabilities/207023

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

Identifikátor

Golang Go - bezpečnostná zraniteľnosť

Popis

Vývojári programovacieho jazyka Golang Go vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

06.08.2021

CVE

CVE-2021-29923

Zasiahnuté systémy

Golang Go 1.16.0

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://github.com/sickcodes/security/blob/master/advisories/SICK-2021-016.md
https://golang.org/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29923
https://exchange.xforce.ibmcloud.com/vulnerabilities/207025

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

Identifikátor

Mitsubishi Electric safety PLCs - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostných zraniteľnostiach produktov Mitsubishi Electric.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom monitoringu sieťovej komunikácie, získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

05.08.2021

CVE

CVE-2021-20594, CVE-2021-20597, CVE-2021-20598

Zasiahnuté systémy

R08/16/32/120SFCPU všetky verzie
R08/16/32/120PSFCPU všetky verzie

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.

Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom 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.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-009_en.pdf
https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-011_en.pdf
https://www.nozominetworks.com/blog/new-research-uncovers-5-vulnerabilities-in-mitsubishi-safety-plcs/
https://thehackernews.com/2021/08/unpatched-security-flaws-expose.html
https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-010_en.pdf

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

Identifikátor

Roxy-WI - bezpečnostná zraniteľnosť

Popis

Autori grafického rozhrania Roxy-WI ku populárnemu reverznému proxy HAProxy vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

07.08.2021

CVE

CVE-2021-38169

Zasiahnuté systémy

Roxy-WI 5.2.2.0
Roxy-WI 5.2.1
Roxy-WI 5.2.0
Roxy-WI 5.1.4.0

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame sledovať webstránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom 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://github.com/hap-wi/roxy-wi/issues/285
https://roxy-wi.org/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38169
https://exchange.xforce.ibmcloud.com/vulnerabilities/206996