BEZPEČNOSTNÝ BULLETIN

Týždeň 30. 12. 2020 - 05. 01. 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-295

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

Identifikátor

Bezpečnostná zraniteľnosť v produktoch Mitsubishi Electric

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.01.2021

CVE

CVE-2020-14496

Zasiahnuté systémy

Mitsubishi Electric CPU Module Logging Configuration Tool vo verzii staršej ako 1.106K
Mitsubishi Electric CW Configurator vo verzii staršej ako 1.011M
Mitsubishi Electric Data Transfer vo verzii staršej ako 3.41T
Mitsubishi Electric EZSocket vo verzii staršej ako 4.6
Mitsubishi Electric FR Configurator2 vo verzii staršej ako 1.23Z
Mitsubishi Electric GT Designer3 Version1 (GOT2000) vo verzii staršej ako 1.236W
Mitsubishi Electric GT SoftGOT1000 Version3 vo verzii staršej ako 3.245F
Mitsubishi Electric GT SoftGOT2000 Version1 vo verzii staršej ako 1.236W
Mitsubishi Electric GX LogViewer vo verzii staršej ako 1.106K
Mitsubishi Electric GX Works2 vo verzii staršej ako 1.595V
Mitsubishi Electric GX Works3 vo verzii staršej ako 1.065T
Mitsubishi Electric M_CommDTM-HART vo verzii staršej ako 1.01B
Mitsubishi Electric MELFA-Works vo verzii staršej ako 4.4
Mitsubishi Electric MELSOFT EM Software Development Kit (EM Configurator) vo verzii staršej ako 1.015R
Mitsubishi Electric Mitsubishi Electric Mitsubishi Electric MELSOFT FieldDeviceConfigurator vo verzii staršej ako 1.04E
Mitsubishi Electric MELSOFT Navigator vo verzii staršej ako 2.70Y
Mitsubishi Electric MH11 SettingTool Version2 vo verzii staršej ako 2.003D
Mitsubishi Electric Mitsubishi Electric Motorizer vo verzii staršej ako 1.010L
Mitsubishi Electric MR Configurator2 vo verzii staršej ako 1.106L
Mitsubishi Electric MT Works2 vo verzii staršej ako 1.160S
Mitsubishi Electric MX Component vo verzii staršej ako 4.20W
Mitsubishi Electric PX Developer vo verzii staršej ako 1.53F
Mitsubishi Electric RT ToolBox2 vo verzii staršej ako 3.73B
Mitsubishi Electric RT ToolBox3 vo verzii staršej ako 1.80J

Následky
Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému Eskalácia privilégií Zneprístupnenie služby Neoprávnený prístup k citlivým údajom Neoprávnená zmena v systéme

Odporúčania
Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. 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://us-cert.cisa.gov/ics/advisories/icsa-20-212-02

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Viacero zraniteľností v Yokogawa CENTUM

Popis

Spoločnosť Yokogawa vydala bezpečnostné aktualizácie pre svoje portfólio produktov, ktoré opravujú dve bezpečnostné zraniteľnosti.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente, prostredníctvom zasielania špeciálne upravených paketov vykonať neoprávnené zmeny v systéme a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

05.01.2021

CVE

CVE-2020-5608, CVE-2020-5609

Zasiahnuté systémy

Exaopc R3.72.00 - R3.78.00 vo verzii staršej ako R3.78.10
CENTUM CS 3000 (vrátane CENTUM CS 3000 Entry Class) R3.08.10 – R3.09.50 a CENTUM VP (vrátane CENTUM VP Entry Class) vo verzii R4.01.00 – R4.03.00 (vrátane) verzie už nie sú podporované
CENTUM VP (vrátane CENTUM VP Entry Class) verzie R5.01.00 – R5.04.20 vo verzii staršej ako R5.04.D1
CENTUM VP (vrátane CENTUM VP Entry Class) verzie R6.01.00 – R6.07.00 vo verzii staršej ako R6.07.11
B/M9000CS R5.04.01 – R5.05.01 s nainštalovaným softvérom CENTUM CS 3000
B/M9000 VP R6.01.01 – R8.03.01 s nainštalovaným softvérom CENTUM CS 3000
Presný popis verzií sa nachádza na adrese
https://us-cert.cisa.gov/ics/advisories/icsa-20-224-01

Následky

Vykonanie škodlivého kódu
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
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://us-cert.cisa.gov/ics/advisories/icsa-20-224-01

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Red Lion Crimson

Popis

Spoločnosť Red Lion vydala bezpečnostnú aktualizáciu na svoj produkt Crimson, ktorá opravuje bezpečnostnú zraniteľnosť.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

05.01.2021

CVE

CVE-2020-27279, CVE-2020-27283, CVE-2020-27285

Zasiahnuté systémy

Crimson 3.1 vo verzii staršej ako 3119.001

Následky

Zneprístupnenie služby
Neoprávnená zmena v systéme
Neoprávnený prístup k citlivým údajom

Odporúčania

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

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-005-04

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Panasonic FPWIN Pro

Popis

Spoločnosť Panasonic vydala bezpečnostnú aktualizáciu na svoj produkt FPWIN Pro, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

05.01.2021

CVE

CVE-2020-16236

Zasiahnuté systémy

Panasonic FPWIN Pro vo verzii staršej ako 7.5.1.0

Následky

Vykonanie škodlivého kódu

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://us-cert.cisa.gov/ics/advisories/icsa-21-005-02
https://isssource.com/panasonic-fixes-fpwin-pro-hole/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.1**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť v produktoch Johnson Controls

Popis

Spoločnosť Sensormatic Electronics, LLC dcérska spoločnosť Johnson Controls vydala bezpečnostné aktualizácie na svoje produkty victor Web Client a C•CURE WebClient, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente, spôsobiť znepristupnenie služby a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

05.01.2021

CVE

CVE-2020-9048

Zasiahnuté systémy

American Dynamics victor Web Client: verzie staršie ako a vrátane 5.4.1
Software House C•CURE Web Client: verzie staršie ako a vrátane 2.80

Následky

Znepristupnenie služby
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-20-282-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.3
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bezpečnostné zraniteľnosti v portfóliu produktov Schneider Electric Modicon

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje viacero bezpečnostných zraniteľností.
Zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, autentifikovanému útočníkovi s používateľskými právomocami vykonať škodlivý kód a následne spôsobiť zneprístupnenie služby a neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

05.01.2021

CVE

CVE-2020-7562, CVE-2020-7563, CVE-2020-7564

Zasiahnuté systémy

M340 CPU BMX P34x, všetky verzie
M340 Komunikačné ethernetové moduly BMX NOE 0100 (H) (všetky verzie), BMX NOE 0110 (H) (všetky verzie), BMX NOC 0401 (všetky verzie), BMX NOR 0200H (všetky verzie)
Prémiové procesory s integrovaným Ethernet COPRO TSXP574634, TSXP575634, TSXP576634 (všetky verzie)
Prémiové komunikačné moduly TSXETY4103 (všetky verzie), TSXETY5103 (všetky verzie)
Quantum procesory s integrovaným Ethernet COPRO 140CPU65xxxxx (všetky verzie)
Quantum komunikačné moduly 140NOE771x1 (všetky verzie), 140NOC78x00 (všetky verzie), 140NOC77101 (všetky verzie)

Následky

Vykonanie škodlivého kódu
Zneprístupnenie služby
Neoprávnená zmena v systéme

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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://us-cert.cisa.gov/ics/advisories/icsa-21-005-01