# BEZPEČNOSTNÝ BULLETIN

Týždeň 01. 11. 2023 - 07. 11. 2023

## 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:
01794/2022/SK-CERT-1400

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

## Identifikátor

BOSCH produkty - viacero bezpečnostných zraniteľností

## Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktov SICK Flexi Soft Gateway a ctrlX HMI Web Panel - WR21.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených paketov získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

24.10.2023

## CVE

CVE-2023-41255, CVE-2023-41372, CVE-2023-41960, CVE-2023-43488, CVE-2023-45220, CVE-2023-45321, CVE-2023-45844, CVE-2023-45851, CVE-2023-46102, CVE-2023-5246

## Zasiahnuté systémy

SICK Flexi Soft Gateway vo všetkých verziách
ctrlX HMI Web Panel - WR21 vo všetkých verziách

## Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

## Odporúčania

Na uvedené zrateniľnosti v v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov. Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu.

## Zdroje

https://psirt.bosch.com/security-advisories/bosch-sa-164691.html
https://psirt.bosch.com/security-advisories/bosch-sa-175607.html

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

## Identifikátor

Red Lion Crimson - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Red Lion vydala bezpečnostnú aktualizáciu na svoj produkt Crimson configuration tool, 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

02.11.2023

## CVE

CVE-2023-5719

## Zasiahnuté systémy

Crimson configuration tool vo verzii staršej ako 3.2.0063

## Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

## 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.

## Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-306-01

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

## Identifikátor

VMware Workspace ONE UEM console a Tools - tri bezpečnostné zraniteľnosti

## Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na produkty Workspace ONE UEM console a Tools, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v nástroji Workspace ONE UEM console, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného odkazu získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

31.10.2023

## CVE

CVE-2023-20886, CVE-2023-34057, CVE-2023-34058

## Zasiahnuté systémy

VMware Tools pre macOS vo verzii staršej ako 12.1.1
VMware Tools pre Windows vo verzii staršej ako 12.3.5
Workspace ONE UEM 2302 vo verzii staršej ako 23.2.0.10
Workspace ONE UEM 2212 vo verzii staršej ako 22.12.0.20
Workspace ONE UEM 2209 vo verzii staršej ako 22.9.0.29
Workspace ONE UEM 2206 vo verzii staršej ako 22.6.0.36
Workspace ONE UEM 2203 vo verzii staršej ako 22.3.0.48

## Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému

## 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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

## Zdroje

https://www.vmware.com/security/advisories/VMSA-2023-0025.html
https://www.vmware.com/security/advisories/VMSA-2023-0024.html

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

## Identifikátor

Franklin Fueling System TS-550 - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Franklin Fueling System vydala bezpečnostnú aktualizáciu na svoj produkt TS-550, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi dekódovať prihlasovacie údaje administrátora a získať tak neoprávený prístup do systému.

## Dátum prvého zverejnenia varovania

02.11.2023

## CVE

CVE-2023-5846

## Zasiahnuté systémy

TS-550 vo verzii staršej ako 1.9.23.8960

## Následky

Neoprávnený prístup do systému
Úplné narušenie dôvernosti, integrity a dostupnosti systému

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

## Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-306-04

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

## Identifikátor

NVIDIA - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie na svoje portfólio ovládačov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

01.11.2023

## CVE

CVE-2023-31016, CVE-2023-31017, CVE-2023-31018, CVE-2023-31019, CVE-2023-31020, CVE-2023-31021, CVE-2023-31022, CVE-2023-31023, CVE-2023-31026, CVE-2023-31027

## Zasiahnuté systémy

GeForce
Studio
NVIDIA RTX
Quadro
NVS
Tesla

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v časti ZDROJE

## Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému

## 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.

## Zdroje

https://nvidia.custhelp.com/app/answers/detail/a_id/5491

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

## Identifikátor

MOXA produkty - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť MOXA vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

02.11.2023

## CVE

CVE-2005-4900, CVE-2015-9251, CVE-2016-0800, CVE-2019-11358, CVE-2020-11022, CVE-2020-11023, CVE-2023-4217, CVE-2023-4452, CVE-2023-5035, CVE-2023-5627

## Zasiahnuté systémy

NPort 6000 Series vo verzii firmvéru staršej ako v2.0
EDR-810 Series vo verzii firmvéru staršej ako v5.12.29
EDR-G902 Series vo verzii firmvéru staršej ako v5.7.21
EDR-G903 Series vo verzii firmvéru staršej ako v5.7.21
PT-G503 Series vo verzii firmvéru staršej ako v5.3

## Následky

Neoprávnený prístup do systému
Neoprávnený prístup k citlivým údajom
Vykonanie škodlivého kódu
Zneprístupnenie služby

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom alebo vykonanie škodlivého kódu 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.moxa.com/en/support/product-support/security-advisory/mpsa-232905-nport-6000-series-incorrect-implementation-of-authentication-algorithm-vulnerability
https://www.moxa.com/en/support/product-support/security-advisory/mpsa-234880-edr-810-g902-g903-series-web-server-buffer-overflow-vulnerability
https://www.moxa.com/en/support/product-support/security-advisory/mpsa-230203-pt-g503-series-multiple-vulnerabilities

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

## Identifikátor

MELSEC iQ-F Series CPU Module - bezpečnostná zraniteľnosť

## Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu MELSEC iQ-F Series CPU Module.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

02.11.2023

## CVE

CVE-2023-4625

## Zasiahnuté systémy

MELSEC CPU moduly série iQ-F vo všetkých verziách
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v časti ZDROJE.

## Následky

Zneprístupnenie služby

## Odporúčania

Administrátorom odporúčame postupovať podľa pokynov výrobcu, ktoré môžete nájsť na webovej adrese:
https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-014_en.pdf
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

## Zdroje

https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-014_en.pdf
https://www.cisa.gov/news-events/ics-advisories/icsa-23-306-02