BEZPEČNOSTNÝ BULLETIN

Týždeň 28. 06. 2023 - 04. 07. 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-1210

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

Identifikátor

NETGEAR Routre - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť NETGEAR vydala bezpečnostné aktualizácie na svoje portfólio routrov, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.06.2023

CVE

CVE-2023-35721, CVE-2023-35722

Zasiahnuté systémy

RAX30 vo verzii firmvéru staršej ako 1.0.11.96_2_HOTFIX
RAX50 vo verzii firmvéru staršej ako 1.0.15.128

Následky

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

Odporúčania

Administrátorom a používateľom 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://kb.netgear.com/000065699/Security-Advisory-for-Pre-Authentication-Command-Injection-on-the-RAX30-PSV-2023-0046
https://kb.netgear.com/000065668/Security-Advisory-for-Improper-Remote-Server-Certificate-Validation-on-the-RAX50-PSV-2023-0019
https://exchange.xforce.ibmcloud.com/vulnerabilities/259544
https://www.zerodayinitiative.com/advisories/ZDI-23-893/
https://www.zerodayinitiative.com/advisories/ZDI-23-894/

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

Identifikátor

D-Link DIR-X3260 - bezpečnostná zraniteľnosť

Popis

Spoločnosť D-Link vydala bezpečnostnú aktualizáciu firvméru pre svoj router DIR-X3260, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód v kontexte root s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.06.2023

CVE

CVE-2023-35723

Zasiahnuté systémy

DIR-X3260 vo verzii firmvéru staršej ako v1.04B01 Beta-Hotfix

Následky

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

Odporúčania

Administrátorom a používateľom 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://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10345
https://www.zerodayinitiative.com/advisories/ZDI-23-892/

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

Identifikátor

Bosch BIS - bezpečnostná zraniteľnosť

Popis

Spoločnosť Bosch vydala bezpečnostnú aktualizáciu na svoj produkt BOSCH-SA-988400-BT, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

28.06.2023

CVE

CVE-2023-29241

Zasiahnuté systémy

BIS 5.0 vo verzii staršej ako patch BIS_5_0_21100_0_Patch1.zip

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

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://psirt.bosch.com/security-advisories/bosch-sa-988400-bt.html

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

Identifikátor

Schneider Electric EcoStruxure Operator Terminal Expert VXDZ - bezpečnostná zraniteľnosť

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoj produkt EcoStruxure Operator Terminal Expert VXDZ, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.06.2023

CVE

CVE-2023-1049

Zasiahnuté systémy

EcoStruxure Operation Terminal Expert vo verzii staršej ako v3.4

Následky

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

Odporúčania

Administrátorom a používateľom 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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-180-02

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

Identifikátor

TN-5900 Series - bezpečnostná zraniteľnosť

Popis

Spoločnosť MOXA vydala bezpečnostnú aktualizáciu na svoj router TN-5900, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom brute force útoku získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

03.06.2023

CVE

CVE-2023-3336

Zasiahnuté systémy

TN-5900 Series vo verzii firmvéru staršej ako 3.4

Následky

Neoprávnený prístup k citlivým údajom

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.moxa.com/en/support/product-support/security-advisory/mpsa-230401-tn-5900-series-user-enumeration-vulnerability

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

Identifikátor

GitLab - viacero bezpečnostných zraniteľností

Popis

Vývojári platformy GitLab vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

29.06.2023

CVE

CVE-2023-0838, CVE-2023-1936, CVE-2023-2190, CVE-2023-2200, CVE-2023-2576, CVE-2023-2620, CVE-2023-3102, CVE-2023-3362, CVE-2023-3363, CVE-2023-3424, CVE-2023-3444

Zasiahnuté systémy

GitLab Community Edition (CE) a Enterprise Edition (EE) vo verzii staršej ako 16.1.1, 16.0.6 a 15.11.10

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://about.gitlab.com/releases/2023/06/29/security-release-gitlab-16-1-1-released/

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

Identifikátor

NVIDIA Produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie na produkty DGX A100, DGX A800 a CUDA Toolkit, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia kritická bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.06.2023

CVE

CVE-2021-26316, CVE-2021-26328, CVE-2021-26402, CVE-2021-39298, CVE-2022-23813, CVE-2022-23814, CVE-2022-26872, CVE-2022-2827, CVE-2022-40242, CVE-2022-40259, CVE-2023-25521, CVE-2023-25522

Zasiahnuté systémy

NVIDIA DGX A100 s SBIOS vo verzii staršej ako 1.21 a s BMC vo verzii staršej ako 00.20.04
NVIDIA DGX A800 s SBIOS vo verzii staršej ako 1.21 a s BMC vo verzii staršej ako 00.20.04
CUDA Toolkit vo verzii staršej ako v12.2

Následky

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

Odporúčania

Administrátorom a používateľom 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://nvidia.custhelp.com/app/answers/detail/a_id/5461
https://nvidia.custhelp.com/app/answers/detail/a_id/5469

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

Identifikátor

Mitsubishi Electric MELSEC-F Series - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu MELSEC-F od spoločnosti Mitsubishi Electric.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených paketov získať neoprávnený prístup do systému a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

29.06.2023

CVE

CVE-2023-2846

Zasiahnuté systémy

FX3U-xMy/z x=16,32,48,64,80,128, y=T,R, z=ES,ESS,DS,DSS *1 vo všetkých verziách
FX3U-32MR/UA1, FX3U-64MR/UA1 *1 vo všetkých verziách
FX3U-32MS/ES, FX3U-64MS/ES *1 vo všetkých verziách
FX3U-xMy/ES-A x=16,32,48,64,80,128, y=T,R *1*2 vo všetkých verziách
FX3UC-xMT/z x=16,32,64,96, z=D,DSS *1 vo všetkých verziách
FX3UC-16MR/D-T, FX3UC-16MR/DS-T *1 vo všetkých verziách
FX3UC-32MT-LT, FX3UC-32MT-LT-2 *1 vo všetkých verziách
FX3UC-16MT/D-P4, FX3UC-16MR/DSS-P4 *1*2 vo všetkých verziách
FX3G-xMy/z x=14,24,40,60, y=T,R, z=ES,ESS,DS,DSS *1 vo všetkých verziách
FX3G-xMy/ES-A x=14,24,40,60, y=T,R *1*2 vo všetkých verziách
FX3GC-32MT/D, FX3GC-32MT/DSS *1 vo všetkých verziách
FX3GE-xMy/z x=24,40, y=T,R, z=ES,ESS,DS,DSS *2 vo všetkých verziách
FX3GA-xMy-CM x=24,40,60, y=T,R *1*2 vo všetkých verziách
FX3S-xMy/z x=10,14,20,30, y=T,R, z=ES,ESS,DS,DSS *1 vo všetkých verziách
FX3S-30My/z-2AD y=T,R, z=ES,ESS *1 vo všetkých verziách
FX3SA-xMy-CM x=10,14,20,30, y=T,R *1*2 vo všetkých verziách

Následky

Neoprávnený prístup do systému
Neoprávnená zmena v systéme

Odporúčania
Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať. 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/2023-005_en.pdf https://www.cisa.gov/news-events/ics-advisories/icsa-23-180-04

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

Identifikátor

Ovarro TBox RTUs - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Ovarro vydala bezpečnostné aktualizácie na svoje portfólio vzdialených koncových jednotiek TBox, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom injekcie škodlivého skriptu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.06.2023

CVE

CVE-2023-3395, CVE-2023-36607, CVE-2023-36608, CVE-2023-36609, CVE-2023-36610, CVE-2023-36611

Zasiahnuté systémy

Vzdialené koncové jednotky Ovarro TBox LT2, MS-CPU32, MS-CPU32-S2, RM2, TG2

Kompletnú špecifikáciu zasiahnutých produktov nájdete na odkaze v časti ZDROJE.

Následky

Neoprávnený prístup k citlivým údajom
Eskalácia privilégií
Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom 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.
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-23-180-03

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 4.0
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Hitachi Energy FOXMAN-UN a UNEM Produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Hitachi Energy vydala bezpečnostné aktualizácie na produkty FOXMAN-UN a UNEM, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom injekcie škodlivého obsahu získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

27.06.2023

CVE

CVE-2023-1711

Zasiahnuté systémy

FOXMAN-UN
UNEM

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v časti ZDROJE

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať.
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. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://search.abb.com/library/Download.aspx?DocumentID=8DBD000155
https://search.abb.com/library/Download.aspx?DocumentID=8DBD000166
https://www.cisa.gov/news-events/ics-advisories/icsa-23-178-01