BEZPEČNOSTNÝ BULLETIN

Týždeň 15. 03. 2023 - 21. 03. 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-1078

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

Identifikátor

Mozilla Firefox - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Mozilla 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 podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.03.2023

CVE

CVE-2023-25748, CVE-2023-25749, CVE-2023-25750, CVE-2023-25751, CVE-2023-25752, CVE-2023-28159, CVE-2023-28160, CVE-2023-28161, CVE-2023-28162, CVE-2023-28163, CVE-2023-28164, CVE-2023-28176, CVE-2023-28177

Zasiahnuté systémy

Thunderbird 102.9
Firefox 111
Firefox ESR 102.9

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

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2023-10/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-09/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-11/

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

Identifikátor

Netgear RAX30 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Netgear vydala bezpečnostnú aktualizáciu na svoj WiFi router AX2400 RAX30, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom a následne vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

14.03.2023

CVE

CVE-2023-1327

Zasiahnuté systémy

AX2400 WiFi Router RAX30 vo verzii staršej ako 1.0.6.74

Následky

Neoprávnený prístup do systému
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://exchange.xforce.ibmcloud.com/vulnerabilities/250089

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

Identifikátor

TP-Link Archer AX21 - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť TP-Link vydala bezpečnostnú aktualizáciu na svoj router Archer AX21, ktorá opravuje dve bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.03.2023

CVE

CVE-2023-27332, CVE-2023-27333

Zasiahnuté systémy

Archer AX21 vo verzii staršej ako 3.6_230219

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://exchange.xforce.ibmcloud.com/vulnerabilities/250275
https://exchange.xforce.ibmcloud.com/vulnerabilities/250273

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

Identifikátor

Zoom produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Zoom Video Communications vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente zrealizovať MITM (Man In The Middle) útok a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.03.2023

CVE

CVE-2023-22881, CVE-2023-22882, CVE-2023-22883, CVE-2023-22884, CVE-2023-22885, CVE-2023-28596, CVE-2023-28597

Zasiahnuté systémy

Zoom Client for Meetings for IT Admin macOS installers before version 5.13.5
Zoom Client for Meetings for IT Admin Windows installers before version 5.13.5
Zoom (for Android, iOS, Linux, macOS, and Windows) clients before version 5.13.5
Zoom Rooms (for Android, iOS, Linux, macOS, and Windows) clients before version 5.13.5
Zoom VDI Windows Meeting clients before version 5.13.10

Následky

Neoprávnený prístup do systému
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://explore.zoom.us/en/trust/security/security-bulletin/

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

Identifikátor

Phoenix Contact ENERGY AXC PU - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Phoenix Contact vydala bezpečnostnú aktualizáciu na svoj produkt ENERGY AXC PU, ktorá opravuje viacero bezpečnostných zraniteľností v komponentoch CODESYS.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

14.03.2023

CVE

CVE-2022-22513, CVE-2022-22514, CVE-2022-22515, CVE-2022-22517, CVE-2022-30792

Zasiahnuté systémy

ENERGY AXC PU vo verzii staršej ako V04.15.00.00

Následky

Neoprávnený prístup k citlivým údajom
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.
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://cert.vde.com/en/advisories/VDE-2023-003/
https://dam-mdc.phoenixcontact.com/asset/156443151564/0a870ae433c19148b80bd760f3a1c1f2/107913_en_03.pdf

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

Identifikátor

GE Digital iFIX - bezpečnostná zraniteľnosť

Popis

Spoločnosť GE Digital vydala bezpečnostnú aktualizáciu na svoj produkt iFIX, ktorá opravuje bezpečnostnú zraniteľnosť.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.03.2023

CVE

CVE-2023-0598

Zasiahnuté systémy

Proficy iFIX vo verzii staršej ako 2023

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

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-073-03

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

Identifikátor

Autodesk FBX SDK - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Autodesk vydala bezpečnostné aktualizácie na produkty KeyShot a FBX SDK, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených FBX súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.03.2023

CVE

CVE-2022-41302, CVE-2022-41303, CVE-2022-41304

Zasiahnuté systémy

KeyShot vo verzii staršej ako 2023.1
Autodesk vo verzii staršej ako FBX SDK 2020.3.2

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
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-23-073-02

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

Identifikátor

Trend Micro Worry-Free Business Security - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Trend Micro vydala bezpečnostné aktualizácie na produkty Worry-Free Business Security Advanced a Worry-Free Business Security Services, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvorených súborov eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

13.03.2023

CVE

CVE-2022-45797, CVE-2023-25144, CVE-2023-25145, CVE-2023-25146, CVE-2023-25147, CVE-2023-25148

Zasiahnuté systémy

WFBS vo verzii staršej ako 10.0 SP1 Patch 2459

WFBSS vo verzii staršej ako February 2023 Monthly Patch (6.7.3107 / 14.2.3044)

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://success.trendmicro.com/dcx/s/solution/000292454?language=en_US

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

Identifikátor

Lenovo produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Lenovo vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť nachádzajúca sa v produkte XClarity Controller (XCC) spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej API požiadavky eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

14.03.2023

CVE

CVE-2022-3728, CVE-2022-4568, CVE-2022-4573, CVE-2022-4574, CVE-2022-4575, CVE-2022-48182, CVE-2022-48183, CVE-2022-48189, CVE-2023-0683, CVE-2023-25492, CVE-2023-25495

Zasiahnuté systémy

Lenovo System Update application vo verzii staršej ako 5.08.01
Lenovo XClarity Controller (XCC)
Lenovo BIOS
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Bezpečnostná záplata je obsiahnutá v aktualizácii UEFI BIOS, preto používateľom odporúčame nainštalovať aktualizácie systému UEFI BIOS z webových stránok výrobcu pre ich konkrétne elektronické zariadenie.
V prípade, že prevádzkujete fyzické servery s operačným systémom Linux, uistite sa, že máte nainštalovaný balík intel-microcode. Na BSD systémoch môžete použiť balík cpupdate.
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://support.lenovo.com/us/en/product_security/LEN-99936
https://support.lenovo.com/us/en/product_security/LEN-103545
https://support.lenovo.com/us/en/product_security/LEN-106014
https://exchange.xforce.ibmcloud.com/vulnerabilities/250233

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

Identifikátor

HPE OneView, FlexNetwork and FlexFabric - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostné aktualizácie na produkty FlexFabric, FlexNetwork a OneView, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa získať úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

16.03.2023

CVE

CVE-2022-28624, CVE-2022-37935

Zasiahnuté systémy

HPE FlexFabric 5700 Switch Series vo verzii staršej ako R2432P61
HPE FlexFabric 5710 Switch Series vo verzii staršej ako R6710
HPE FlexFabric 5930 Switch Series vo verzii staršej ako R2432P61
HPE FlexFabric 5940 Switch Series vo verzii staršej ako R6710
HPE FlexFabric 5945 Switch Series vo verzii staršej ako R6710
HPE FlexNetwork 5130 EI Switch Series vo verzii staršej ako R3507P08
HPE FlexNetwork 10500 Switch Series vo verzii staršej ako R7634P09
HPE OneView for VMware for vCenter (OV4VC) vo verzii staršej ako 11.3.

Následky

Neoprávnený prístup do systému
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://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04449en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04265en_us

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

Identifikátor

MOXA UC Series - bezpečnostná zraniteľnosť

Popis

Spoločnosť MOXA vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi s fyzickým prístupom k zariadeniu získať neoprávnený prístup do systému a úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

14.03.2023

CVE

CVE-2023-1257

Zasiahnuté systémy

UC-8580 Series vo verzii staršej ako V1.1
UC-8540 Series vo verzii staršej ako V1.2
UC-8410A Series vo verzii staršej ako V2.2
UC-8200 Series vo verzii staršej ako V2.4
UC-8100A-ME-T Series vo verzii staršej ako V1.1
UC-8100 Series vo verzii staršej ako V1.2
UC-5100 Series vo verzii staršej ako V1.2
UC-3100 Series vo verzii staršej ako V2.0
UC-2100 Series vo verzii staršej ako V1.5
UC-2100-W Series vo verzii staršej ako V1.5

Následky

Neoprávnený prístup do systému
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.moxa.com/en/support/product-support/security-advisory/uc-series-improper-physical-access-control-vulnerability

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

Identifikátor

Codesys V3 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Codesys vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
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

08.03.2023

CVE

CVE-2022-47391

Zasiahnuté systémy

CODESYS Control RTE (SL) vo verzii staršej ako V3.5.19.0
CODESYS Control RTE (for Beckhoff CX) SL vo verzii staršej ako V3.5.19.0
CODESYS Control Win (SL) vo verzii staršej ako V3.5.19.0
CODESYS Runtime Toolkit vo verzii staršej ako V3.5.19.0
CODESYS Safety SIL2 Runtime Toolkit vo verzii staršej ako V3.5.19.0
CODESYS Safety SIL2 PSP vo verzii staršej ako V3.5.19.0
CODESYS Edge Gateway for Windows vo verzii staršej ako V3.5.19.0
CODESYS Gateway vo verzii staršej ako V3.5.19.0
CODESYS HMI (SL) vo verzii staršej ako V3.5.19.0
CODESYS Development System V3 vo verzii staršej ako V3.5.19.0
CODESYS Control for BeagleBone SL vo verzii staršej ako V4.8.0.0
CODESYS Control for emPC-A/iMX6 SL vo verzii staršej ako V4.8.0.0
CODESYS Control for IOT2000 SL vo verzii staršej ako V4.8.0.0
CODESYS Control for Linux SL vo verzii staršej ako V4.8.0.0
CODESYS Control for PFC100 SL vo verzii staršej ako V4.8.0.0
CODESYS Control for PFC200 SL vo verzii staršej ako V4.8.0.0
CODESYS Control for PLCnext SL vo verzii staršej ako V4.8.0.0
CODESYS Control for Raspberry Pi SL vo verzii staršej ako V4.8.0.0
CODESYS Control for WAGO Touch Panels 600 SL vo verzii staršej ako V4.8.0.0
CODESYS Edge Gateway for Linux vo verzii staršej ako V4.8.0.0

Následky

Zneprístupnenie služby

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://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17555&token=212fc7e39bdd260cab6d6ca84333d42f50bcb3da&download=

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

Identifikátor

Dell BIOS - bezpečnostná zraniteľnosť

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu BIOS pre svoj produkt Embedded Box PC 3000, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.03.2023

CVE

CVE-2023-24571

Zasiahnuté systémy

Embedded Box PC 3000 s BIOS update vo verzii staršej ako 1.18.0

Následky

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

Odporúčania

Bezpečnostná záplata je obsiahnutá v aktualizácii UEFI BIOS, preto používateľom odporúčame nainštalovať aktualizácie systému UEFI BIOS z webových stránok výrobcu pre ich konkrétne elektronické zariadenie.
V prípade, že prevádzkujete fyzické servery s operačným systémom Linux, uistite sa, že máte nainštalovaný balík intel-microcode. Na BSD systémoch môžete použiť balík cpupdate.
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://exchange.xforce.ibmcloud.com/vulnerabilities/250320