BEZPEČNOSTNÝ BULLETIN

Týždeň 01. 03. 2023 - 07. 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-1057

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

Identifikátor

Firefox for Android - bezpečnostná zraniteľnosť

Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu na svoj produkt Firefox for Android.
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

28.02.2023

CVE

CVE-2023-25747

Zasiahnuté systémy

Firefox pre Android vo verzii staršej ako 110.1.0

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://www.mozilla.org/en-US/security/advisories/mfsa2023-08/
https://exchange.xforce.ibmcloud.com/vulnerabilities/248617

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

Identifikátor

ABB S+ Operations - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti HMI S+ Operations.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje neautentifikovanému útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme alebo spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.02.2023

CVE

CVE-2023-0228

Zasiahnuté systémy

S+ Operations vo všetkých verziách

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

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.
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://search.abb.com/library/Download.aspx?DocumentID=7PAA006722&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.79210064.572052908.1677675919-1784065056.1661159789

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

Identifikátor

Phoenix Contact Cloud Client & TC Router - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Phoenix Contact vydala bezpečnostné aktualizácie na svoje Cloud klienty a TC routre, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.03.2023

CVE

CVE-2023-0861, CVE-2023-0862

Zasiahnuté systémy

CLOUD CLIENT 2002T-4G EU vo verzii staršej ako 4.5.73.107
CLOUD CLIENT 2002T-WLAN vo verzii staršej ako 4.5.73.107
CLOUD CLIENT 2102T-4G EU WLAN vo verzii staršej ako 4.5.73.107
TC ROUTER 4002T-4G EU vo verzii staršej ako 4.5.72.107
TC ROUTER 4102T-4G EU WLAN vo verzii staršej ako 4.5.72.107
TC ROUTER 4202T-4G EU WLAN vo verzii staršej ako 4.5.72.107

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://cert.vde.com/en/advisories/VDE-2022-053/

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

Identifikátor

Google Android - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj operačný systém Android, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.03.2023

CVE

CVE-2021-33655, CVE-2022-20467, CVE-2022-20499, CVE-2022-22075, CVE-2022-25655, CVE-2022-25694, CVE-2022-25705, CVE-2022-25709, CVE-2022-33213, CVE-2022-33242, CVE-2022-33244, CVE-2022-33250, CVE-2022-33254, CVE-2022-33256, CVE-2022-33272, CVE-2022-33278, CVE-2022-33309, CVE-2022-40515, CVE-2022-40527, CVE-2022-40530, CVE-2022-40531, CVE-2022-40535, CVE-2022-40537, CVE-2022-40540, CVE-2022-4452, CVE-2022-47459, CVE-2022-47460, CVE-2022-47461, CVE-2022-47462, CVE-2023-20620, CVE-2023-20621, CVE-2023-20623, CVE-2023-20906, CVE-2023-20910, CVE-2023-20911, CVE-2023-20917, CVE-2023-20926, CVE-2023-20929, CVE-2023-20931, CVE-2023-20936, CVE-2023-20947, CVE-2023-20951, CVE-2023-20952, CVE-2023-20953, CVE-2023-20954, CVE-2023-20955, CVE-2023-20956, CVE-2023-20957, CVE-2023-20958, CVE-2023-20959, CVE-2023-20960, CVE-2023-20962, CVE-2023-20963, CVE-2023-20964, CVE-2023-20966

Zasiahnuté systémy

Google Android vo verzii staršej ako patch úroveň 2023-03-05

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://source.android.com/docs/security/bulletin/2023-03-01
https://www.cybersecurity-help.cz/vulnerabilities/72868/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

TPM 2.0 - dve bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach modulu TPM 2.0.
Najzávažnejšia 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

28.02.2023

CVE

CVE-2023-1017, CVE-2023-1018

Zasiahnuté systémy

TPM 2.0 vo všetkých verziách

Následky

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

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.
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://trustedcomputinggroup.org/wp-content/uploads/TCGVRT0007-Advisory-FINAL.pdf
https://trustedcomputinggroup.org/resource/errata-for-tpm-library-specification-2-0/
https://securityonline.info/two-security-flaws-cve-2023-1017-cve-2023-1018-found-on-trusted-platform-module-2-0/

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

Identifikátor

systemd - bezpečnostná zraniteľnosť

Popis

Vývojári balíka systemd pre operačné systémy Linux vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.03.2023

CVE

CVE-2023-26604

Zasiahnuté systémy

systemd vo verzii staršej ako 247

Následky

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.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/249251
https://github.com/systemd/systemd

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

Identifikátor

Hitachi Energy Gateway Station - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Hitachi Energy vydala bezpečnostnú aktualizáciu na svoj produkt Gateway Station, 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

28.02.2023

CVE

CVE-2020-25692, CVE-2022-0778, CVE-2022-1778, CVE-2022-2277, CVE-2022-29492, CVE-2022-29922

Zasiahnuté systémy

Hitachi Gateway Station (GWS) vo verzii staršej ako 3.3.0.0

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://www.cisa.gov/news-events/ics-advisories/icsa-23-059-02
https://www.cisa.gov/news-events/ics-advisories/icsa-23-059-01

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

Identifikátor

Mitsubishi Electric MELSEC iQ-F produkty - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktov rady MELSEC iQ-F.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implemetnácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

02.03.2023

CVE

CVE-2023-0457

Zasiahnuté systémy

FX5U(C) CPU moduly, všetky modely vo všetkých verziách
FX5UJ CPU moduly, všetky modely vo všetkých verziách
FX5S CPU moduly, všetky modely vo všetkých verziách
FX5-ENET vo všetkých verziách
FX5-ENET/IP vo všetkých verziách

Následky

Neoprávnený prístup k citlivým údajom

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.
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://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf
https://www.cisa.gov/news-events/ics-advisories/icsa-23-061-01

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

Identifikátor

DrayTek routre - bezpečnostná zraniteľnosť

Popis

Spoločnosť DrayTek vydala bezpečnostné aktualizácie na svoje portfólio routrov Vigor, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom XSS (Cross Site Scripting) útoku získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

02.03.2023

CVE

CVE-2023-23313

Zasiahnuté systémy

Vigor3910 vo verzii firmvéru staršej ako 4.3.2.2
Vigor3220 Series vo verzii firmvéru staršej ako 3.9.7.4
Vigor2962 Series vo verzii firmvéru staršej ako 4.3.2.2
Vigor1000B vo verzii firmvéru staršej ako 4.3.2.2
Vigor2952 / 2952P vo verzii firmvéru staršej ako 3.9.7.4
Vigor2927 Series vo verzii firmvéru staršej ako 4.4.2.3
Vigor2927 LTE Series vo verzii firmvéru staršej ako 4.4.2.3
Vigor2926 Series vo verzii firmvéru staršej ako 3.9.9.1
Vigor2926 LTE Series vo verzii firmvéru staršej ako 3.9.9.1
Vigor2925 Series vo verzii firmvéru staršej ako 3.9.4
Vigor2925 LTE Series vo verzii firmvéru staršej ako 3.9.4
Vigor2915 Series vo verzii firmvéru staršej ako 4.4.2.1
Vigor2866 Series vo verzii firmvéru staršej ako 4.4.1.1

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.

Zdroje
https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/ https://exchange.xforce.ibmcloud.com/vulnerabilities/249178