BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 04. 2023 - 12. 04. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Hitachi Vantara - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	Cisco produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Mozilla Firefox - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	Mitsubishi Electric, Factory Automation Engineering producty - bezpečnostná zraniteľnosť	Vysoká	**8.3**
05.	Envoy Proxy - viacero bezpečnostných zraniteľností	Vysoká	**8.2**
06.	G Data Total Security - bezpečnostná zraniteľnosť	Vysoká	**7.8**
07.	Acuant AcuFill a AsureID - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
08.	Justsystems produkty - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
09.	FANUC ROBOGUIDE-HandlingPRO - bezpečnostná zraniteľnosť	Stredná	**6.8**
10.	QNAP produkty - tri bezpečnostné zraniteľnosti	Stredná	**6.5**

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-1091

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

Identifikátor

Hitachi Vantara - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Hitachi vydala bezpečnostné aktualizácie na svoj produkt Business Analytics Server, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov vzdialený neautentifikovaný útočník by ju prostredníctvom zaslania špeciálne vytvorenej požiadavky mohol zneužiť na získanie neoprávneného prístupu do systému.
Ostatné zraniteľnosti by vzdialený autentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

03.04.2023

CVE

CVE-2022-43769, CVE-2022-43771, CVE-2022-43772, CVE-2022-43773, CVE-2022-43938, CVE-2022-43939, CVE-2022-43940, CVE-2022-43941

Zasiahnuté systémy

Hitachi Vantara Pentaho Business Analytics Server vo verziách starších ako 9.4.0.1 a 9.3.0.2

Následky

Neoprávnený prístup do systému
Eskalácia privilégií
Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
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://support.pentaho.com/hc/en-us/sections/360010039791-Security-Updates
https://exchange.xforce.ibmcloud.com/vulnerabilities/251769
https://exchange.xforce.ibmcloud.com/vulnerabilities/251770
https://exchange.xforce.ibmcloud.com/vulnerabilities/251766
https://exchange.xforce.ibmcloud.com/vulnerabilities/251771
https://exchange.xforce.ibmcloud.com/vulnerabilities/251768
https://exchange.xforce.ibmcloud.com/vulnerabilities/251764
https://exchange.xforce.ibmcloud.com/vulnerabilities/251772
https://exchange.xforce.ibmcloud.com/vulnerabilities/251763

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-1091

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

Identifikátor

Cisco produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť nachádzajúca sa v produkte Cisco Secure Network Analytics spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.04.2023

CVE

CVE-2023-02121, CVE-2023-20051, CVE-2023-20096, CVE-2023-20102, CVE-2023-20103, CVE-2023-20117, CVE-2023-20121, CVE-2023-20122, CVE-2023-20123, CVE-2023-20124, CVE-2023-20127, CVE-2023-20128, CVE-2023-20129, CVE-2023-20130, CVE-2023-20131, CVE-2023-20132, CVE-2023-20134, CVE-2023-20137, CVE-2023-20138, CVE-2023-20139, CVE-2023-20152, CVE-2023-20153

Zasiahnuté systémy
Cisco PGW vo verzii staršej ako 21.28.0 Cisco Duo for macOS Two-Factor Authentication Software vo verzii staršej ako 2.0.1 Cisco Duo Authentication for Windows Logon and RDP Software vo verzii staršej ako 4.2.2 Cisco ISE 3.2 vo verzii staršej ako 3.2P1 Cisco Prime Infrastructure 3.7 vo verzii staršej ako 3.7.1 update 07 (Apr 2023) Cisco Prime Infrastructure 3.8 vo verzii staršej ako 3.8.1 update 04 (Apr 2023) Cisco Prime Infrastructure 3.9 vo verzii staršej ako 3.9.1 update 03 (Apr 2023) Cisco Prime Infrastructure 3.1 vo verzii staršej ako 3.10.4 Cisco EPNM 5 vo verzii staršej ako 5.0.2.5 Cisco EPNM 5.1 vo verzii staršej ako 5.1.4.3 Cisco EPNM 6 vo verzii staršej ako 6.0.2.1 Cisco EPNM 6.1 vo verzii staršej ako 6.1.1.1 Cisco EPNM 7.0.0 vo verzii staršej ako 7.0.1 RV016 Multi-WAN VPN routre vo všetkých verziách (end of life) RV042 Dual WAN VPN routre vo všetkých verziách (end of life) RV042G Dual Gigabit WAN VPN routre vo všetkých verziách (end of life) RV082 Dual WAN VPN routre vo všetkých verziách (end of life) RV160 VPN routre vo všetkých verziách (end of life) RV160W Wireless-AC VPN routre vo všetkých verziách (end of life) RV260 VPN routre vo všetkých verziách (end of life) RV260P VPN routre with PoE vo všetkých verziách (end of life) RV260W Wireless-AC VPN routre vo všetkých verziách (end of life) RV340 Dual WAN Gigabit VPN routre vo všetkých verziách (end of life) RV340W Dual WAN Gigabit Wireless-AC VPN routre vo všetkých verziách (end of life) RV345 Dual WAN Gigabit VPN routre vo všetkých verziách (end of life) RV345P Dual WAN Gigabit PoE VPN routre vo všetkých verziách (end of life) Cisco Secure Network Analytics vo verzii staršej ako 7.4.2 Cisco Unified CCX vo verzii staršej ako 12.5(1)SU3

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-stealthsmc-rce-sfNBPjcS https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-pdng-dos-KmzwEy2Q https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-2XbOg9Dg https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-stealth-rce-BDwXFK9C https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uccx-xss-GO9L9xxr https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wbx-sxss-fupl-64uHbcm5 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv01x_rv32x_rce-nzAGWWDD https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-adeos-MLAyEcvk https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv32x-cmdinject-cKQsZpxL

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 spôsobiť pretečenie zásobníka a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

11.04.2023

CVE

CVE-2023-0547, CVE-2023-1945, CVE-2023-28163, CVE-2023-29479, CVE-2023-29531, CVE-2023-29532, CVE-2023-29533, CVE-2023-29534, CVE-2023-29535, CVE-2023-29536, CVE-2023-29537, CVE-2023-29538, CVE-2023-29539, CVE-2023-29540, CVE-2023-29541, CVE-2023-29542, CVE-2023-29543, CVE-2023-29544, CVE-2023-29545, CVE-2023-29546, CVE-2023-29547, CVE-2023-29548, CVE-2023-29549, CVE-2023-29550, CVE-2023-29551

Zasiahnuté systémy

Mozilla Firefox vo verzii staršej ako 112
Mozilla Firefox pre Android vo verzii staršej ako 112
Mozilla Focus pre Android vo verzii staršej ako 112
Mozilla Firefox ESR vo verzii staršej ako 102.10
Mozilla Thunderbird vo verzii staršej ako 102.10

Následky

Vykonanie škodlivého kódu

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/mfsa2023-13/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-14/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-15/

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

Identifikátor

Mitsubishi Electric, Factory Automation Engineering producty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosit systému.

Dátum prvého zverejnenia varovania

11.04.2023

CVE

CVE-2020-14521

Zasiahnuté systémy
C Controller Interface Module utility vo verzii staršej ako 2.10
CC-Link IE Control Network Data Collector vo verzii staršej ako 1.01B
CC-Link IE Field Network Data Collector vo verzii staršej ako 1.01B
CC-Link IE TSN Data Collector vo verzii staršej ako 1.01B
CPU Module Logging Configuration Tool vo verzii staršej ako 1.106K
CW Configurator vo verzii staršej ako 1.011M
Data Transfer vo verzii staršej ako 3.43V
EZSocket vo verzii staršej ako 5.2
FR Configurator2 vo verzii staršej ako 1.27D
GT Designer3 Version1(GOT1000) vo verzii staršej ako 1.245F
GT Designer3 Version1(GOT2000) vo verzii staršej ako 1.245F
GT SoftGOT1000 Version3 vo verzii staršej ako 3.245F
GT SoftGOT2000 Version1 vo verzii staršej ako 1.245F
GX Developer vo verzii staršej ako 8.505B
GX LogViewer vo verzii staršej ako 1.106K
GX Works2 vo verzii staršej ako 1.605F
GX Works3 vo verzii staršej ako 1.065T
M_CommDTM-IO-Link vo verzii staršej ako 1.04E
MELFA-Works vo verzii staršej ako 4.5
MELSOFT Complete Clean Up Tool vo verzii staršej ako 1.07H
MELSOFT EM Software Development Kit vo verzii staršej ako 1.020W
MELSOFT iQ AppPortal vo verzii staršej ako 1.20W
MELSOFT Navigator vo verzii staršej ako 2.78G
MI Configurator vo verzii staršej ako 1.005F
Motion Control Setting vo verzii staršej ako 1.006G
Motorizer vo verzii staršej ako 1.010L
MR Configurator2 vo verzii staršej ako 1.130L
MT Works2 vo verzii staršej ako 1.170C
MTConnect Data Collector vo verzii staršej ako 1.1.5.0 (*2)
MX Component vo verzii staršej ako 4.21X
MX MESInterface vo verzii staršej ako 1.22Y
MX MESInterface-R vo verzii staršej ako 1.13P
MX Sheet vo verzii staršej ako 2.16S
Network Interface Board CC IE Control Utility vo verzii staršej ako 1.30G
Network Interface Board CC IE Field Utility vo verzii staršej ako 1.17T
Network Interface Board CC-Link Ver.2 Utility vo verzii staršej ako 1.24A
Network Interface Board MNETH Utility vo verzii staršej ako 35M
Position Board utility 2 vo verzii staršej ako 3.30
PX Developer vo verzii staršej ako 1.54G
RT ToolBox2 vo verzii staršej ako 3.74C
RT ToolBox3 vo verzii staršej ako 1.90U
Setting/monitoring tools for the C Controller module (SW3PVC-CCPU) vo verzii staršej ako 3.14Q
Setting/monitoring tools for the C Controller module (SW4PVC-CCPU) vo verzii staršej ako 4.13P
SLMP Data Collector vo verzii staršej ako 1.05F

Následky
Neoprávnený prístup k citlivým informáciám Neoprávnené zmeny v systéme Zneprístupnenie služby Vykonanie škodlivého kódu

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace systémy a jednotky odporúčame prevádzkovať úplne oddelené od internetu. 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 neoprávnený prístup k citlivým informáciám 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.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-007_en.pdf

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

Identifikátor

Envoy Proxy - viacero bezpečnostných zraniteľností

Popis

Vývojári proxy Envoy vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému neautentifikovanému útočníkovi vykonať neoprávnené zmeny v systéme, získať neoprávnený prístup k citlivým údajom alebo spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

04.04.2023

CVE

CVE-2023-27487, CVE-2023-27488, CVE-2023-27491, CVE-2023-27492, CVE-2023-27493, CVE-2023-27496

Zasiahnuté systémy

Envoy vo verzii staršej ako 1.25.3, 1.24.4, 1.23.6, 1.22.9

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.

Zdroje

https://github.com/envoyproxy/envoy/security/advisories/GHSA-5375-pq35-hf2g
https://github.com/envoyproxy/envoy/security/advisories/GHSA-j79q-2g66-2xv5
https://github.com/envoyproxy/envoy/security/advisories/GHSA-9g5w-hqr3-w2ph
https://github.com/envoyproxy/envoy/security/advisories/GHSA-w5w5-487h-qv8q
https://github.com/envoyproxy/envoy/security/advisories/GHSA-wpc2-2jp6-ppg2

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

Identifikátor

G Data Total Security - bezpečnostná zraniteľnosť

Popis

Spoločnosť G Data vydala bezpečnostnú aktualizáciu na svoj produkt Total Security, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.04.2023

CVE

CVE-2023-27347

Zasiahnuté systémy

G Data Total Security vo verzii staršej ako 25.5.13.26

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://www.zerodayinitiative.com/advisories/ZDI-23-379/

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

Identifikátor

Acuant AcuFill a AsureID - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Acuant vydala bezpečnostné aktualizácie na produkty AcuFill a AsureID, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v AcuFill SDK, 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.
Zraniteľnosti v AsureID by lokálny autentifikovaný používateľ mohol zneužiť na eskaláciu privilégií.

Dátum prvého zverejnenia varovania

04.04.2023

CVE

CVE-2022-48221, CVE-2022-48222, CVE-2022-48223, CVE-2022-48224, CVE-2022-48225, CVE-2022-48226, CVE-2022-48227

Zasiahnuté systémy

AcuFill SDK vo verzii staršej ako 10.22.02.03
AsureID Sentinel vo verzii staršej ako 5.2.149

Následky

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

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/251906
https://exchange.xforce.ibmcloud.com/vulnerabilities/251904
https://exchange.xforce.ibmcloud.com/vulnerabilities/251902
https://exchange.xforce.ibmcloud.com/vulnerabilities/251901
https://exchange.xforce.ibmcloud.com/vulnerabilities/251900
https://exchange.xforce.ibmcloud.com/vulnerabilities/251898
https://exchange.xforce.ibmcloud.com/vulnerabilities/251897

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

Identifikátor

Justsystems produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Justsystems vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.04.2023

CVE

CVE-2022-43664, CVE-2022-45115, CVE-2023-22291, CVE-2023-22660

Zasiahnuté systémy

Ichitaro series
Hanako series
Rakuraku Hagaki series
Label Mighty series
JUST Office series
JUST Government series
JUST Police series
Homepage Builder 21

Presnú špecifikáciu zasiahnutých produktov nájdete na webovej adrese:
https://www.justsystems.com/jp/corporate/info/js23001.html

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

http://jvn.jp/en/jp/JVN79149117/index.html
https://www.justsystems.com/jp/corporate/info/js23001.html

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.8
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

FANUC ROBOGUIDE-HandlingPRO - bezpečnostná zraniteľnosť

Popis

Spoločnosť FANUC vydala bezpečnostnú aktualizáciu na svoj produkt ROBOGUIDE-HandlingPRO, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

11.04.2023

CVE

CVE-2023-1864

Zasiahnuté systémy

FANUC ROBOGUIDE-HandlingPRO vo verzii staršej ako 9 Rev.ZD (vrátane)

Následky

Neoprávnený prístup k citlivým informáciám

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace systémy a jednotky odporúčame prevádzkovať úplne oddelené od internetu.
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-23-101-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

QNAP produkty - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť QNAP vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.03.2023

CVE

CVE-2022-27597, CVE-2022-27598, CVE-2023-23355

Zasiahnuté systémy

QuTScloud, QVP (QVR Pro appliances), QVR vo všetkých verziách
QTS vo verzii staršej ako 5.0.1.2346 build 20230322
QuTS hero vo verzii staršej ako h5.0.1.2348 build 20230324

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
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 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.qnap.com/en/security-advisory/qsa-23-10
https://www.qnap.com/en/security-advisory/qsa-23-06
https://nvd.nist.gov/vuln/detail/CVE-2023-23355
https://www.redpacketsecurity.com/qnap-qts-qnap-quts-hero-qnap-qutscloud-qnap-qvp-qvr-pro-appliances-and-qnap-qvr-command-execution-cve-2023-23355-6/
https://sternumiot.com/iot-blog/qnap-ts-230-nas-vulnerability/

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-1091