BEZPEČNOSTNÝ BULLETIN

Týždeň 02. 08. 2023 - 08. 08. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	MLflow - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	HCL Verse - dve bezpečnostné zraniteľnosti	Vysoká	**8.8**
03.	Mozilla produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	TP-Link Archer AX21 - bezpečnostná zraniteľnosť	Vysoká	**8.8**
05.	Aruba CX - bezpečnostná zraniteľnosť	Vysoká	**8.8**
06.	F5 BIG-IP - bezpečnostná zraniteľnosť	Vysoká	**8.8**
07.	CODESYS Development System a Control - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
08.	Splunk SOAR - bezpečnostná zraniteľnosť	Vysoká	**8.6**
09.	PaperCut - tri bezpečnostné zraniteľnosti	Vysoká	**8.4**
10.	Inductive Automation Ignition OPC UA - viacero bezpečnostných zraniteľností	Vysoká	**8.3**
11.	OMRON produkty - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
12.	GitLab - viacero bezpečnostných zraniteľností	Vysoká	**7.5**
13.	pnpm - bezpečnostná zraniteľnosť	Vysoká	**7.5**
14.	SEIKO EPSON printer Web Config - bezpečnostná zraniteľnosť	Vysoká	**7.5**
15.	Mitsubishi Electric GT a GOT Series - dve bezpečnostné zraniteľnosti	Vysoká	**7.5**
16.	TEL-STER TelWin SCADA WebInterface - bezpečnostná zraniteľnosť	Vysoká	**7.5**
17.	Sensormatic Electronics VideoEdge - bezpečnostná zraniteľnosť	Vysoká	**7.1**

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-1268

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

Identifikátor

MLflow - bezpečnostná zraniteľnosť

Popis

Vývojári platformy MLflow 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 vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Na uvedenú zraniteľnosť je voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

31.07.2023

CVE

CVE-2023-4033

Zasiahnuté systémy

MLflow vo verzii staršej ako 2.5.0

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://github.com/mlflow/mlflow/commit/6dde93758d42455cb90ef324407919ed67668b9b
https://exchange.xforce.ibmcloud.com/vulnerabilities/262107
https://huntr.dev/bounties/5312d6f8-67a5-4607-bd47-5e19966fa321/

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

Identifikátor

HCL Verse - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť HCL Software vydala bezpečnostnú aktualizáciu na svoj produkt HCL Verse, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom stored cross-site scripting (XSS) útoku vykonať škodlivý kód a získať neoprávnený prístup k citlivým údajom. Zneužitie zraniteľnosti vyžaduje interakciu obete, ktorá musí otvoriť špeciálne vytvorenú e-mailovú správu.

Dátum prvého zverejnenia varovania

01.08.2023

CVE

CVE-2023-28013, CVE-2023-37496

Zasiahnuté systémy

HCL Verse vo verzii staršej ako 3.1

Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom

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://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0105904
https://exchange.xforce.ibmcloud.com/vulnerabilities/262111

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

Identifikátor

Mozilla produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Mozilla Foundation 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

01.08.2023

CVE

CVE-2023-4045, CVE-2023-4046, CVE-2023-4047, CVE-2023-4048, CVE-2023-4049, CVE-2023-4050, CVE-2023-4051, CVE-2023-4052, CVE-2023-4053, CVE-2023-4054, CVE-2023-4055, CVE-2023-4056, CVE-2023-4057, CVE-2023-4058

Zasiahnuté systémy

Thunderbird vo verzii staršej ako 115.1
Firefox vo verzii staršej ako 116
Firefox ESR vo verzii staršej ako 102.14

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/mfsa2023-31/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-29/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-30/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-33/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-32/

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

Identifikátor

TP-Link Archer AX21 - bezpečnostná zraniteľnosť

Popis

Spoločnosť TP-Link vydala bezpečnostnú aktualizáciu na svoj produkt Archer AX21, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.07.2023

CVE

CVE-2023-31710

Zasiahnuté systémy

Archer AX21 vo verzii firmvéru staršej ako V3.6_230621
Archer AX21 vo verzii firmvéru staršej ako V3_230621

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://www.securitynewspaper.com/2023/08/01/how-to-easily-hack-tp-link-archer-ax21-wi-fi-router/
https://www.tp-link.com/us/support/download/archer-ax21/#Firmware

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

Identifikátor

Aruba CX - bezpečnostná zraniteľnosť

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostnú aktualizáciu na svoje switche CX Aruba, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.08.2023

CVE

CVE-2023-3718

Zasiahnuté systémy

AOS-CX vo verzii staršej ako 10.12.0006
AOS-CX vo verzii staršej ako 10.11.1021
AOS-CX vo verzii staršej ako 10.10.1060

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne 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.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04498en_us

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

Identifikátor

F5 BIG-IP - bezpečnostná zraniteľnosť

Popis

Spoločnosť F5 vydala bezpečnostnú aktualizáciu na svoje portfólio produktov BIG-IP, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom reflected cross-site scripting (XSS) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.08.2023

CVE

CVE-2023-38138

Zasiahnuté systémy

BIG-IP (všetky moduly) vo verzii staršej ako 14.1.5.5, 15.1.9.1, 16.1.3.5, a 17.1.0.2

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://my.f5.com/manage/s/article/K000133474
https://exchange.xforce.ibmcloud.com/vulnerabilities/262308

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

Identifikátor

CODESYS Development System a Control - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach programovateľných radičov CODESYS. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.08.2023

CVE

CVE-2022-4046, CVE-2023-28355, CVE-2023-3662, CVE-2023-3663

Zasiahnuté systémy

CODESYS Control pre PFC200 SL vo všetkých verziách
CODESYS Control pre PLCnext SL vo všetkých verziách
CODESYS Control pre Raspberry Pi SL vo všetkých verziách
CODESYS Control pre WAGO Touch Panels 600 SL vo všetkých verziách
CODESYS Control RTE (pre Beckhoff CX) SL vo všetkých verziách
CODESYS Control RTE (SL) vo všetkých verziách
CODESYS Control Runtime System Toolkit vo všetkých verziách
CODESYS Control Win (SL) vo všetkých verziách
CODESYS HMI (SL) vo všetkých verziách

Následky

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

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. Detailné inštrukcie môžete nájsť na webových stránkach uvedených v časti ZDROJE.

Zdroje

https://cert.vde.com/en/advisories/VDE-2023-025/
https://cert.vde.com/en/advisories/VDE-2023-022/
https://cert.vde.com/en/advisories/VDE-2023-021/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Splunk SOAR - bezpečnostná zraniteľnosť

Popis

Spoločnosť Splunk vydala bezpečnostnú aktualizáciu na svoj produkt SOAR, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

31.07.2023

CVE

CVE-2023-3997

Zasiahnuté systémy

Splunk SOAR (On-premises) vo verzii staršej ako 6.1.0
Splunk SOAR (Cloud) vo verzii staršej ako 6.1.0.131

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://advisory.splunk.com/advisories/SVD-2023-0702

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

Identifikátor

PaperCut - tri bezpečnostné zraniteľnosti

Popis

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

Dátum prvého zverejnenia varovania

04.08.2023

CVE

CVE-2022-21724, CVE-2023-3486, CVE-2023-39143

Zasiahnuté systémy

PaperCut NG/MF vo verzii staršej ako 22.1.3

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.
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.papercut.com/kb/Main/SecurityBulletinJuly2023/
https://www.horizon3.ai/cve-2023-39143-papercut-path-traversal-file-upload-rce-vulnerability/
https://thehackernews.com/2023/08/researchers-uncover-new-high-severity.html

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

Identifikátor

Inductive Automation Ignition OPC UA - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Inductive Automation vydala bezpečnostnú aktualizáciu na svoj produkt Ignition, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom injekcie škodlivého skriptu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu obete.

Dátum prvého zverejnenia varovania

01.08.2023

CVE

CVE-2023-38121, CVE-2023-38122, CVE-2023-38123, CVE-2023-38124

Zasiahnuté systémy

Ignition vo verzii staršej ako 8.1.26

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://www.zerodayinitiative.com/advisories/ZDI-23-1012/
https://www.zerodayinitiative.com/advisories/ZDI-23-1013/
https://www.zerodayinitiative.com/advisories/ZDI-23-1014/
https://www.zerodayinitiative.com/advisories/ZDI-23-1015/

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

Identifikátor

OMRON produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť OMRON vydala bezpečnostné aktualizácie na produkty CX-Programmer a CPU a Ethernet/IP jednotky sérií CS a CJ, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zneužitia out-of-bounds zápisu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.08.2023

CVE

CVE-2023-38744, CVE-2023-38746, CVE-2023-38747, CVE-2023-38748

Zasiahnuté systémy

CX-Programmer V9.81
CJ2M-CPU3 vo verzii staršej ako 2.19
CJ2H-CPU6[]-EIP vo verzii staršej ako 3.05
CS1W-EIP21 vo verzii staršej ako 3.05
CJ1W-EIP21 vo verzii staršej ako 3.05

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom
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.
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.ia.omron.com/product/vulnerability/OMSR-2023-005_en.pdf
http://jvn.jp/en/vu/JVNVU93286117/index.html
http://jvn.jp/en/vu/JVNVU92193064/index.html

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 podvrhnutia špeciálne vytvorených súborov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

01.08.2023

CVE

CVE-2023-0632, CVE-2023-1210, CVE-2023-2022, CVE-2023-2164, CVE-2023-3364, CVE-2023-3385, CVE-2023-3401, CVE-2023-3500, CVE-2023-3900, CVE-2023-3993, CVE-2023-3994, CVE-2023-4002, CVE-2023-4008, CVE-2023-4011

Zasiahnuté systémy

GitLab Community Edition (CE) a Enterprise Edition (EE) vo verzii staršej ako 16.2.2, 16.1.3, a 16.0.8

Následky

Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom
Vykonanie škodlivého kódu

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://about.gitlab.com/releases/2023/08/01/security-release-gitlab-16-2-2-released/

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

Identifikátor

pnpm - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja pre manažment balíkov pnpm vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvorených TAR súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.08.2023

CVE

CVE-2023-37478

Zasiahnuté systémy

pnpm vo verzii staršej ako 7.33.4, 8.6.8

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://github.com/pnpm/pnpm/security/advisories/GHSA-5r98-f33j-g8h7
https://exchange.xforce.ibmcloud.com/vulnerabilities/262181

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

Identifikátor

SEIKO EPSON printer Web Config - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu SEIKO EPSON printer Web Config.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

02.08.2023

CVE

CVE-2023-38556

Zasiahnuté systémy

SEIKO EPSON printer Web Config vo všetkých verziách

Následky

Zneprístupnenie služby

Odporúčania

Výrobca neplánuje vydať bezpečnostné aktualizácie a odporúča tlačiarne prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.epson.jp/support/misc_t/230802_oshirase.htm
http://jvn.jp/en/jp/JVN61337171/index.html

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

Identifikátor

Mitsubishi Electric GT a GOT Series - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Mitsubishi Electri vydala bezpečnostné aktualizácie na svoje portfólio produktov GT a GOT, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom odpočúvania sieťovej prevádzky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

03.08.2023

CVE

CVE-2023-0525, CVE-2023-3373

Zasiahnuté systémy

GT Designer3 Version1 (GOT2000) vo verzii staršej ako v1.300N
GT SoftGOT2000 vo verzii staršej ako v1.300N
GOT2000 (Models GT21, GT23, GT25, GT27) vo verzii staršej ako v01.50.000
GOT SIMPLE (Models GS25, GS21) vo verzii staršej ako v01.50.000
GOT2000 Series, GT21 model vo verzii staršej ako 01.50.000
GOT SIMPLE, GS21 model vo verzii staršej ako 01.50.000

Následky

Neoprávnený prístup k citlivým údajom
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://www.cisa.gov/news-events/ics-advisories/icsa-23-215-02
https://www.cisa.gov/news-events/ics-advisories/icsa-23-215-01

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

Identifikátor

TEL-STER TelWin SCADA WebInterface - bezpečnostná zraniteľnosť

Popis

Spoločnosť TEL-STER vydala bezpečnostné aktualizácie na produkt TelWin SCADA WebInterface, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

03.08.2023

CVE

CVE-2023-0956

Zasiahnuté systémy

TelWin SCADA WebInterface vo verzii staršej ako 6.2, 7.2, 8.1, 9.1, alebo 10.0.

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.cisa.gov/news-events/ics-advisories/icsa-23-215-03

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.1
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Sensormatic Electronics VideoEdge - bezpečnostná zraniteľnosť

Popis

Spoločnosť Sensormatic vydala bezpečnostnú aktualizáciu na svoj produkt Electronics VideoEdge, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

03.08.2023

CVE

CVE-2023-3749

Zasiahnuté systémy

VideoEdge vo verzii staršej ako 6.1.1

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.johnsoncontrols.com/-/media/jci/cyber-solutions/product-security-advisories/2023/jci-psa-2023-07.pdf
https://www.cisa.gov/news-events/ics-advisories/icsa-23-215-04