BEZPEČNOSTNÝ BULLETIN

Týždeň 21. 06. 2023 - 27. 06. 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-1196

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

Identifikátor

Schneider Electric PowerLogic

Popis

Spoločnosť Schneider Electric vydala bezpečnostné aktualizácie na svoje portfólio elektromerov PowerLogic, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom odpočúvania sieťovej prevádzky získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

13.06.2023

CVE

CVE-2022-46680

Zasiahnuté systémy

PowerLogic ION9000 vo verzii staršej ako 4.0.0
PowerLogic ION7400 vo verzii staršej ako 4.0.0
PowerLogic PM8000 vo verzii staršej ako v4.0.0
PowerLogic ION8650 vo všetkých verziách
PowerLogic ION8800 vo všetkých verziách
Legacy verzie produktovej rady ION

Následky

Neoprávnený prístup k citlivým údajom
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-129-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-129-03.pdf
https://thehackernews.com/2023/06/researchers-expose-new-severe-flaws-in.html
https://www.darkreading.com/ics-ot/schneider-power-meter-vulnerability-power-outages
https://nvd.nist.gov/vuln/detail/CVE-2022-46680

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

Identifikátor

Apple produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Apple 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

21.06.2023

CVE

CVE-2023-32434, CVE-2023-32435, CVE-2023-32439

Zasiahnuté systémy

Safari vo verzii staršej ako 16.5.1
watchOS vo verzii staršej ako 8.8.1
watchOS vo verzii staršej ako 9.5.2
macOS Big Sur vo verzii staršej ako 11.7.8
macOS Monterey vo verzii staršej ako 12.6.7
macOS Ventura vo verzii staršej ako 13.4.1
iOS 15.7.7 a iPadOS vo verzii staršej ako 15.7.7
iOS 16.5.1 a iPadOS vo verzii staršej ako 16.5.1

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://support.apple.com/en-us/HT213816
https://support.apple.com/en-us/HT213808
https://support.apple.com/en-us/HT213812
https://support.apple.com/en-us/HT213809
https://support.apple.com/en-us/HT213810
https://support.apple.com/en-us/HT213813
https://support.apple.com/en-us/HT213811
https://support.apple.com/en-us/HT213814
https://exchange.xforce.ibmcloud.com/vulnerabilities/258636

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.7
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Nextcloud Server - bezpečnostná zraniteľnosť

Popis

Vývojári platformy Nextcloud Server vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

22.06.2023

CVE

CVE-2023-32320

Zasiahnuté systémy

Nextcloud Server vo verzii staršej ako 25.0.7 a 26.0.2
Nextcloud Enterprise Server vo verzii staršej ako 21.0.9.12, 22.2.10.12, 23.0.12.7, 24.0.12.2, 25.0.7, a 26.0.2

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://github.com/nextcloud/security-advisories/security/advisories/GHSA-qphh-6xh7-vffg
https://exchange.xforce.ibmcloud.com/vulnerabilities/258746

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

Identifikátor

Enphase Installer & Envoy - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktov Enphase Installer Toolkit a Enphase Envoy.

Bezpečnostná zraniteľnosť v produkte Installer Toolkit spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Bezpečnostná zraniteľnosti v produkte Envoy spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a vzdialený autentifikovaný používateľ s právomocami používateľa by ju mohol zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

22.06.2023

CVE

CVE-2023-32274, CVE-2023-33869

Zasiahnuté systémy

Enphase Installer Toolkit vo verzii staršej ako 3.27.0 (vrátane)
Enphase Envoy vo verzii staršej ako D7.0.88 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom
Vykonanie škodlivého kódu

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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://www.cisa.gov/news-events/ics-advisories/icsa-23-171-02
https://www.cisa.gov/news-events/ics-advisories/icsa-23-171-01

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

Identifikátor

VMware vCenter Server & Cloud Foundation - viacero bezpečnostných zraniteľností

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte vCenter Server, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.06.2023

CVE

CVE-2023-20892, CVE-2023-20893, CVE-2023-20894, CVE-2023-20895, CVE-2023-20896

Zasiahnuté systémy

vCenter Server 8 vo verzii staršej ako 8.0 U1b
vCenter Server 8 vo verzii staršej ako 8.0 U1b
vCenter Server 7 vo verzii staršej ako 7.0 U3m
vCenter Server 7 vo verzii staršej ako 7.0 U3m
Cloud Foundation (vCenter Server) 5.x vo verzii staršej ako 8.0 U1b
Cloud Foundation (vCenter Server) 5.x vo verzii staršej ako 8.0 U1b
Cloud Foundation (vCenter Server) 4.x vo verzii staršej ako 7.0 U3m
Cloud Foundation (vCenter Server) 4.x vo verzii staršej ako 7.0 U3m

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.vmware.com/security/advisories/VMSA-2023-0014.html

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

Identifikátor

Junos OS and Junos OS Evolved - bezpečnostná zraniteľnosť

Popis

Spoločnosť Juniper vydala bezpečnostné aktualizácie na svoje produkty Junos OS a Junos OS Evolved, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

21.06.2023

CVE

CVE-2023-0026

Zasiahnuté systémy

Junos OS vo verzii staršej ako 20.4R3-S8, 21.2R3-S6, 21.3R3-S5, 21.4R3-S4, 22.1R3-S4, 22.2R3-S2, 22.3R2-S2, 22.3R3-S1, 22.4R2-S1, 22.4R3, 23.1R1-S1, 23.1R2, 23.2R1

Junos OS Evolved vo verzii staršej ako 20.4R3-S8-EVO, 21.2R3-S6-EVO, 21.3R3-S5-EVO, 21.4R3-S4-EVO, 22.1R3-S4-EVO, 22.2R3-S2-EVO, 22.3R2-S2-EVO, 22.3R3-S1-EVO, 22.4R2-S1-EVO, 22.4R3-EVO, 23.1R1-S1-EVO, 23.1R2-EVO, 23.2R1-EVO

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://supportportal.juniper.net/s/article/2023-06-Out-of-Cycle-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-A-BGP-session-will-flap-upon-receipt-of-a-specific-optional-transitive-attribute-CVE-2023-0026?language=en_US

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

Identifikátor

ISC BIND - tri bezpečnostné zraniteľnosti

Popis

Vývojári DNS servera BIND vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú tri bezpečnostné zraniteľnosti.
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

21.06.2023

CVE

CVE-2023-2828, CVE-2023-2829, CVE-2023-2911

Zasiahnuté systémy

ISC BIND vo verzii staršej ako 9.16.42, 9.18.16 a 9.19.14

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.openwall.com/lists/oss-security/2023/06/21/6
https://exchange.xforce.ibmcloud.com/vulnerabilities/258607
https://exchange.xforce.ibmcloud.com/vulnerabilities/258609
https://exchange.xforce.ibmcloud.com/vulnerabilities/258648

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

Identifikátor

Apache Tomcat - bezpečnostná zraniteľnosť

Popis

Vývojári servletu Apache Tomcat vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

21.06.2023

CVE

CVE-2023-34981

Zasiahnuté systémy

Apache Tomcat vo verzii staršej ako 11.0.0-M6
Apache Tomcat vo verzii staršej ako 10.1.9
Apache Tomcat vo verzii staršej ako 9.0.75
Apache Tomcat vo verzii staršej ako 8.5.89

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://lists.apache.org/thread/j1ksjh9m9gx1q60rtk1sbzmxhvj5h5qz
https://exchange.xforce.ibmcloud.com/vulnerabilities/258638

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

Identifikátor

WAGO: Series 750-3x/-8x - bezpečnostná zraniteľnosť

Popis

Spoločnosť WAGO vydala bezpečnostné aktualizácie na svoje portfólio modulov WAGO série 750, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

25.06.2023

CVE

CVE-2023-1150

Zasiahnuté systémy

WAGO 750-332 vo verzii staršej ako FW11 po BACnet certifikácií
WAGO 750-362/xxx-xxx vo verzii staršej ako FW11 Q3/2023
WAGO 750-363/xxx-xxx vo verzii staršej ako FW11 Q3/2023
WAGO 750-364/xxx-xxx vo verzii staršej ako FW11 Q3/2023
WAGO 750-365/xxx-xxx vo verzii staršej ako FW11 Q3/2023
WAGO 750-823 vo verzii staršej ako FW11 Q3/2023
WAGO 750-832/xxx-xxx vo verzii staršej ako FW11 po BACnet certifikácií
WAGO 750-862 vo verzii staršej ako FW11 Q1/2023
WAGO 750-890/xxx-xxx vo verzii staršej ako FW11 Q3/2023
WAGO 750-891 vo verzii staršej ako FW11 Q3/2023
WAGO 750-893 vo verzii staršej ako FW11 Q3/2023

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://cert.vde.com/en/advisories/VDE-2023-005/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.3**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Cloudflare WARP client - bezpečnostná zraniteľnosť

Popis

Spoločnosť Cloudflare vydala bezpečnostnú aktualizáciu na svoj produkt WARP client for Windows, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.06.2023

CVE

CVE-2023-1862

Zasiahnuté systémy

WARP client for Windows vo verzii staršej ako 2023.3.381.0

Následky

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://github.com/cloudflare/advisories/security/advisories/GHSA-q55r-53c8-5642
https://exchange.xforce.ibmcloud.com/vulnerabilities/258502

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

Identifikátor

NVIDIA Jetson Series - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie na svoje portfólio výpočtových platforiem Jetson, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi s fyzickým prístupom k zariadeniu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.06.2023

CVE

CVE-2023-25518, CVE-2023-25520

Zasiahnuté systémy

Jetson AGX Xavier series, Jetson Xavier NX, Jetson TX2 series a Jetson TX2 NX vo verzii staršej ako 32.7.4

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.

Zdroje

https://nvidia.custhelp.com/app/answers/detail/a_id/5466

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 4.9
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SpiderControl SCADAWebServer - bezpečnostná zraniteľnosť

Popis

Spoločnosť SpiderControl vydala bezpečnostnú aktualizáciu na svoj produkt SCADAWebServer, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom podvrhnutia špeciálne vytvorených súborov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

22.06.2023

CVE

CVE-2023-3329

Zasiahnuté systémy

SCADAWebServer vo verzii staršej ako 2.09

Následky

Zneprístupnenie služby

Odporúčania

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

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-173-03