BEZPEČNOSTNÝ BULLETIN

Týždeň 12. 04. 2023 - 18. 04. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	Phoenix Contact ENERGY AXC PU - bezpečnostná zraniteľnosť	Vysoká	**8.8**
03.	Firefox, Thunderbird - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	Schneider Electric produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
05.	Korenix Jetwave - tri bezpečnostné zraniteľnosti	Vysoká	**8.8**
06.	Cisco - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
07.	Juniper produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.2**
08.	HPE OneView & OneView Global Dashboard - viacero bezpečnostných zraniteľností	Vysoká	**7.9**
09.	JTEKT ELECTRONICS Produkty - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
10.	Datakit CrossCAD/Ware - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
11.	Mitsubishi Electric India GC-ENET-COM - bezpečnostná zraniteľnosť	Vysoká	**7.5**
12.	ROBOGUIDE-HandlingPRO - bezpečnostná zraniteľnosť	Stredná	**6.8**

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-1100

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

Identifikátor

Google Chrome - bezpečnostná zraniteľnosť

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač Chrome, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v JavaScript engine V8 a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

11.04.2023

CVE

CVE-2023-2033

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 112.0.5615.121

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://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_14.html
https://thehackernews.com/2023/04/google-releases-urgent-chrome-update-to.html
https://www.suse.com/security/cve/CVE-2023-2033.html

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

Identifikátor

Phoenix Contact ENERGY AXC PU - bezpečnostná zraniteľnosť

Popis

Spoločnosť Phoenix Contact vydala bezpečnostnú aktualizáciu na svoju webovú službu ENERGY AXC PU, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom špeciálne vytvorenej URL získať úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

11.04.2023

CVE

CVE-2023-1109

Zasiahnuté systémy

ENERGY AXC PU vo verzii staršej ako V04.15.00.01
SMARTRTU AXC SG vo verzii staršej ako V01.09.00.00
SMARTRTU AXC IG vo verzii staršej ako V01.02.00.01 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
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 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://cert.vde.com/en/advisories/VDE-2023-004/

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

Identifikátor

Firefox, Thunderbird - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Mozilla Foundation vydala bezpečnostné aktualizácie na svoje produkty, 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

11.04.2023

CVE

CVE-2023-0547, CVE-2023-1945, CVE-2023-1999, 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

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

Následky

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 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.mozilla.org/en-US/security/advisories/mfsa2023-15/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-14/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-13/
https://access.redhat.com/security/cve/CVE-2023-29533

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

Identifikátor

Schneider Electric produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Schneider Electric vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v CODESYS Runtime, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

11.04.2023

CVE

CVE-2022-34755, CVE-2022-4046, CVE-2022-4224, CVE-2023-1548, CVE-2023-25619, CVE-2023-25620, CVE-2023-27976, CVE-2023-28355, CVE-2023-29410, CVE-2023-29411, CVE-2023-29412, CVE-2023-29413

Zasiahnuté systémy

PacDrive 3 Controllers LMC
Eco/Pro/Pro2
PacDrive Controller LMC078
Modicon Controller M241
Modicon Controller M251
Modicon Controller M262
Modicon Controller M258
Modicon Controller LMC058
Modicon Controller M218
HMISCU Controller
Easergy Builder installer
EcoStruxure™ Control Expert
APC Easy UPS
Schneider Electric Easy UPS
InsightHome
InsightFacility
Conext™ Gateway (Discontinued in 2019)
Modicon M580 (part numbers BMEP* and BMEH*, excluding M580 CPU Safety)
Modicon Modicon M340 CPU (part numbers BMXP34*)

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

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. 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_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-01.pdf&p_Doc_Ref=SEVD-2023-101-01 https://download.schneider-electric.com/files?p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-06.pdf&p_Doc_Ref=SEVD-2023-101-06 https://download.schneider-electric.com/files?p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-03.pdf&p_Doc_Ref=SEVD-2023-101-03 https://download.schneider-electric.com/files?p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf&p_Doc_Ref=SEVD-2023-101-04 https://download.schneider-electric.com/files?p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-02.pdf&p_Doc_Ref=SEVD-2023-101-02 https://download.schneider-electric.com/files?p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-05.pdf&p_Doc_Ref=SEVD-2023-101-05

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

Identifikátor

Korenix Jetwave - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Korenix vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
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

06.04.2023

CVE

CVE-2023-23294, CVE-2023-23295, CVE-2023-23296

Zasiahnuté systémy

Korenix JetWave 4221 HP-E s firmvérom starším ako verzia V1.4.0
Korenix JetWave 2212G s firmvérom starším ako verzia V1.10
Korenix JetWave 2212X s firmvérom starším ako verzia V1.11
Korenix JetWave 2112S s firmvérom starším ako verzia V1.11
Korenix JetWave 2211C s firmvérom starším ako verzia V1.6
Korenix JetWave 2411/2111 s firmvérom starším ako verzia V1.5
Korenix JetWave 2411L/2111L s firmvérom starším ako verzia V1.6
Korenix JetWave 2414/2114 s firmvérom starším ako verzia V1.4
Korenix JetWave 2424 s firmvérom starším ako verzia V1.3
Korenix JetWave 2460 s firmvérom starším ako verzia V1.6
Korenix JetWave 3220 V3 s firmvérom starším ako verzia V1.7
Korenix JetWave 3420 V3 s firmvérom starším ako verzia V1.7

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
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.
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.cisa.gov/news-events/ics-advisories/icsa-23-096-04

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

Identifikátor

Cisco - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť nachádzajúca sa Cisco IOS a IOS XE spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne upravených SNMP paketov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

17.04.2023

CVE

CVE-2017-6736, CVE-2017-6737, CVE-2017-6738, CVE-2017-6739, CVE-2017-6740, CVE-2017-6741, CVE-2017-6742, CVE-2017-6743, CVE-2017-6744, CVE-2023-20127, CVE-2023-20129, CVE-2023-20130, CVE-2023-20131

Zasiahnuté systémy

Cisco Evolved Programmable Network Manager
Cisco IOS and IOS XE Software
Cisco Prime Infrastructure
Cisco EPNM

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe

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

Identifikátor

Juniper produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Juniper vydala bezpečnostné aktualizácie na svoje portfólio produktov, 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 vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.04.2023

CVE

CVE-2023-1697, CVE-2023-22394, CVE-2023-22396, CVE-2023-28959, CVE-2023-28960, CVE-2023-28961, CVE-2023-28962, CVE-2023-28963, CVE-2023-28964, CVE-2023-28965, CVE-2023-28966, CVE-2023-28967, CVE-2023-28968, CVE-2023-28970, CVE-2023-28973, CVE-2023-28974, CVE-2023-28975, CVE-2023-28976, CVE-2023-28978, CVE-2023-28979, CVE-2023-28980, CVE-2023-28981, CVE-2023-28982, CVE-2023-28983, CVE-2023-28984

Zasiahnuté systémy

Junos OS
Junos OS Evolved

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE.

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. V prípade, že aktualizácia systému nie je možná, odporúčame postupovať podľa pokynov výrobcu uvedených na odkazoch v sekcii ZDROJE.
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://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-QFX10000-Series-PTX1000-Series-The-dcpfe-process-will-crash-when-a-malformed-ethernet-frame-is-received-CVE-2023-1697?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-SRX-Series-and-MX-Series-Memory-leak-due-to-receipt-of-specially-crafted-SIP-calls-CVE-2023-22394?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Paragon-Active-Assurance-Enabling-the-

timescaledb-enables-IP-forwarding-CVE-2023-28971?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-Evolved-Shell-Injection-vulnerability-in-the-gNOI-server-CVE-2023-28983?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-NFX-Series-set-system-ports-console-insecure-allows-root-password-recovery-CVE-2023-28972?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-SRX-Series-Policies-that-rely-on-JDPI-Decoder-actions-may-fail-open-CVE-2023-28968?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-Evolved-Read-access-to-some-confidential-user-information-is-possible-CVE-2023-28978?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-JRR200-Kernel-crash-upon-receipt-of-a-specific-packet-CVE-2023-28970?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-Evolved-Local-low-privileged-user-with-shell-access-can-execute-CLI-commands-as-root-CVE-2023-28966?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-QFX10002-Failure-of-storm-control-feature-may-lead-to-Denial-of-Service-CVE-2023-28965?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Malformed-BGP-flowspec-update-causes-RPD-crash-CVE-2023-28964?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-An-attacker-sending-genuine-BGP-packets-causes-an-RPD-crash-CVE-2023-28967?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-QFX10002-PFE-wedges-and-restarts-upon-receipt-of-specific-malformed-packets-CVE-2023-28959?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-Evolved-The-sysmanctl-shell-command-allows-a-local-user-to-gain-access-to-some-administrative-actions-CVE-2023-28973?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-Evolved-Docker-repository-is-world-writeable-allowing-low-privileged-local-user-to-inject-files-into-Docker-containers-CVE-2023-28960?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-MX-Series-In-a-BBE-scenario-upon-receipt-of-specific-malformed-packets-from-subscribers-the-process-bbe-smgd-will-crash-CVE-2023-28974?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-QFX-Series-The-PFE-may-crash-when-a-lot-of-MAC-addresses-are-being-learned-and-aged-CVE-2023-28984?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-The-kernel-will-crash-when-certain-USB-devices-are-inserted-CVE-2023-28975?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-MX-Series-If-a-specific-traffic-rate-goes-above-the-DDoS-threshold-it-will-lead-to-an-FPC-crash-CVE-2023-28976?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-In-a-6PE-scenario-upon-receipt-of-a-specific-IPv6-packet-an-integrity-check-fails-CVE-2023-28979?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-In-a-BGP-rib-sharding-scenario-an-rpd-crash-will-happen-shortly-after-a-specific-CLI-command-is-issued-CVE-2023-28980?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-In-a-BGP-rib-sharding-scenario-when-a-route-is-frequently-updated-an-rpd-memory-leak-will-occur-CVE-2023-28982?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-If-malformed-IPv6-router-advertisements-are-received-memory-corruption-will-occur-which-causes-an-rpd-crash-CVE-2023-28981?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-Multiple-vulnerabilities-in-J-Web?language=en_US
https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-ACX-Series-IPv6-firewall-filter-is-not-installed-in-PFE-when-from-next-header-ah-is-used-CVE-2023-28961?language=en_US

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.9
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

HPE OneView & OneView Global Dashboard - viacero bezpečnostných zraniteľností

Popis

Spoločnosť HPE vydala bezpečnostné aktualizácie na produkty OneView a OneView Global Dashboard, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú lokálnemu, autentifikovanému útočníkovi s právomocami používateľa získať neoprávnený prístup k citlivým údajom, ktoré by mohli byť zneužité na následné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.04.2023

CVE

CVE-2023-28084, CVE-2023-28085, CVE-2023-28086, CVE-2023-28087, CVE-2023-28088, CVE-2023-28089, CVE-2023-28090, CVE-2023-28091

Zasiahnuté systémy

HPE OneView Global Dashboard vo verzii staršej ako 2.72
HPE OneView vo verzii staršej ako 8.2
HPE OneView vo verzii staršej ako 6.60.04 LTS

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom 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=hpesbgn04468en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04467en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04469en_us

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

Identifikátor

JTEKT ELECTRONICS Produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť JTEKT ELECTRONICS vydala bezpečnostné aktualizácie na produkty Kostac PLC Programing Software a Screen Creator Advance 2, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.04.2023

CVE

CVE-2023-22345, CVE-2023-22346, CVE-2023-22347, CVE-2023-22349, CVE-2023-22350, CVE-2023-22353, CVE-2023-22360, CVE-2023-22419, CVE-2023-22421, CVE-2023-22424

Zasiahnuté systémy

JTEKT ELECTRONICS Kostac PLC Programing Software vo verzii staršej ako 1.6.10.0
JTEKT ELECTRONICS Screen Creator Advance 2 vo verzii staršej ako Ver.0.1.1.4 Build01A

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.
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.
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.cisa.gov/news-events/ics-advisories/icsa-23-096-02
https://www.cisa.gov/news-events/ics-advisories/icsa-23-096-03

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

Identifikátor

Datakit CrossCAD/Ware - viacero bezpečnostných zraniteľností

Popis

Spoločnosť DATAKIT vydala bezpečnostnú aktualizáciu na svoj konverzný nástroj CrossCAD/Ware_x64 library, ktorá opravuje 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

13.04.2023

CVE

CVE-2023-22295, CVE-2023-22321, CVE-2023-22354, CVE-2023-22846, CVE-2023-23579

Zasiahnuté systémy

CrossCAD/Ware_x64 library vo verzii staršej ako v2023.1

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.cisa.gov/news-events/ics-advisories/icsa-23-103-14

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

Identifikátor

Mitsubishi Electric India GC-ENET-COM - bezpečnostná zraniteľnosť

Popis

Spoločnosť Mitsubishi Electric India vydala bezpečnostnú aktualizáciu na svoj produkt GC-ENET-COM, ktorá opravuje 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

13.04.2023

CVE

CVE-2023-1285

Zasiahnuté systémy

GC-ENET-COM zariadenia, ktorých firmvér začína sériovým číslom nižším ako 17

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-23-103-15

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

Identifikátor

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 prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

11.04.2023

CVE

CVE-2023-1864

Zasiahnuté systémy

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

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-23-101-01