BEZPEČNOSTNÝ BULLETIN

Týždeň 19. 07. 2023 - 25. 07. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Zyxel produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Foxit Reader - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	Apple produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
05.	Avaya Aura - bezpečnostná zraniteľnosť	Vysoká	**8.6**
06.	MS Edge - bezpečnostná zraniteľnosť	Vysoká	**8.1**
07.	WellinTech KingHistorian - dve bezpečnostné zraniteľnosti	Vysoká	**8.1**
08.	OpenSSH - bezpečnostná zraniteľnosť	Vysoká	**8.1**
09.	Atlassian Confluence Data Center & Server, Bamboo - tri bezpečnostné zraniteľnosti	Vysoká	**8.0**
10.	Keysight N6845A - tri bezpečnostné zraniteľnosti	Vysoká	**7.8**
11.	Rockwell Automation Kinetix 5700 - bezpečnostná zraniteľnosť	Vysoká	**7.5**
12.	Crestron 3-Series - bezpečnostná zraniteľnosť	Vysoká	**7.5**
13.	GE Digital CIMPLICITY - bezpečnostná zraniteľnosť	Stredná	**6.6**

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-1244

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

Identifikátor

Zyxel produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Zyxel vydala bezpečnostné aktualizácie na svoje portfólio firewallov a sieťových prvkov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne vytvorených konfiguračných príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.07.2023

CVE

CVE-2023-28767, CVE-2023-33011, CVE-2023-33012, CVE-2023-34138, CVE-2023-34139, CVE-2023-34140, CVE-2023-34141

Zasiahnuté systémy

NXC2500 vo verzii staršej ako V6.10(AAIG.3) (vrátane)
NXC5500 vo verzii staršej ako V6.10(AAOS.4) (vrátane)
ATP vo verzii staršej ako ZLD V5.37
USG FLEX vo verzii staršej ako ZLD V5.37
USG FLEX 50(W) / USG20(W)-VPN vo verzii staršej ako ZLD V5.37
VPN vo verzii staršej ako ZLD V5.37

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Pre získanie aktualizačných súborov pre NXC2500 a NXC5500 je nutné kontaktovať zákaznícku podporu firmy Zyxel.
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.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers
https://nvd.nist.gov/vuln/detail/CVE-2023-33011

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

Identifikátor

Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostné aktualizácie na internetové prehliadače Chrome pre Windows, Mac a Linux, 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

18.07.2023

CVE

CVE-2023-3727, CVE-2023-3728, CVE-2023-3730, CVE-2023-3732, CVE-2023-3733, CVE-2023-3734, CVE-2023-3735, CVE-2023-3736, CVE-2023-3737, CVE-2023-3738, CVE-2023-3740

Zasiahnuté systémy

Chrome pre Linux a Mac vo verzii staršej ako 115.0.5790.98
Chrome pre Windows vo verzii staršej ako 115.0.5790.98/99

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://chromereleases.googleblog.com/2023/07/stable-channel-update-for-desktop.html

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

Identifikátor

Foxit Reader - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Foxit Software vydala bezpečnostnú aktualizáciu na svoj produkt Foxit Reader, ktorá opravuje viacero bezpečnostných zraniteľností.
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.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

19.07.2023

CVE

CVE-2023-27379, CVE-2023-28744, CVE-2023-32664, CVE-2023-33866, CVE-2023-33876

Zasiahnuté systémy

Foxit Reader vo verzii staršej ako 12.1.3.15356

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://talosintelligence.com/vulnerability_reports/TALOS-2023-1757
https://talosintelligence.com/vulnerability_reports/TALOS-2023-1795
https://talosintelligence.com/vulnerability_reports/TALOS-2023-1796
https://talosintelligence.com/vulnerability_reports/TALOS-2023-1756
https://talosintelligence.com/vulnerability_reports/TALOS-2023-1739

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.
Zraniteľnosti sú v súčasnosti aktívne zneužívané útočníkmi.

Dátum prvého zverejnenia varovania

24.07.2023

CVE

CVE-2023-23540, CVE-2023-28319, CVE-2023-28320, CVE-2023-28321, CVE-2023-28322, CVE-2023-2953, CVE-2023-32364, CVE-2023-32381, CVE-2023-32409, CVE-2023-32416, CVE-2023-32418, CVE-2023-32429, CVE-2023-32433, CVE-2023-32437, CVE-2023-32441, CVE-2023-32442, CVE-2023-32443, CVE-2023-32734, CVE-2023-35983, CVE-2023-35993, CVE-2023-36854, CVE-2023-36862, CVE-2023-37450, CVE-2023-38133, CVE-2023-38136, CVE-2023-38258, CVE-2023-38259, CVE-2023-38261, CVE-2023-38410, CVE-2023-38421, CVE-2023-38424, CVE-2023-38425, CVE-2023-38564, CVE-2023-38565, CVE-2023-38572, CVE-2023-38580, CVE-2023-38593, CVE-2023-38594, CVE-2023-38595, CVE-2023-38597, CVE-2023-38600, CVE-2023-38602, CVE-2023-38603, CVE-2023-38606, CVE-2023-38608, CVE-2023-38611

Zasiahnuté systémy

Safari vo verzii staršej ako 16.6
iOS vo verzii staršej ako 15.7.8
iPadOS vo verzii staršej ako 15.7.8
iOS vo verzii staršej ako 16.6
iPadOS vo verzii staršej ako 16.6
macOS Ventura vo verzii staršej ako 13.5
macOS Monterey vo verzii staršej ako 12.6.8
macOS Big Sur vo verzii staršej ako 11.7.9
tvOS vo verzii staršej ako 16.6
watchOS vo verzii staršej ako 9.6

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/kb/HT213841 https://support.apple.com/kb/HT213842 https://support.apple.com/kb/HT213843 https://support.apple.com/kb/HT213844 https://support.apple.com/kb/HT213845 https://support.apple.com/kb/HT213846 https://support.apple.com/kb/HT213847 https://support.apple.com/kb/HT213848

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

Identifikátor

Avaya Aura - bezpečnostná zraniteľnosť

Popis

Spoločnosť Avaya vydala bezpečnostnú aktualizáciu na svoj produkt Avaya Aura, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.07.2023

CVE

CVE-2023-3722

Zasiahnuté systémy

Avaya Aura vo verzii staršej ako 8.1.4.1

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.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/261173

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

Identifikátor

MS Edge - bezpečnostná zraniteľnosť

Popis

Spoločnosť Microsoft vydala bezpečnostné aktualizácie na svoj internetový prehliadač Edge, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených PDF súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

17.07.2023

CVE

CVE-2023-36887

IOC

-

Zasiahnuté systémy

Microsoft Edge (Chromium-based) vo verzii staršej ako 114.0.1823.82

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://talosintelligence.com/vulnerability_reports/TALOS-2023-1747
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36887

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

Identifikátor

WellinTech KingHistorian - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť WellinTech vydala bezpečnostnú aktualizáciu na svoj produkt KingHistorian, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených paketov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.07.2023

CVE

CVE-2022-43663, CVE-2022-45124

Zasiahnuté systémy

KingHistorian vo verzii staršej ako V3.52

Následky

Neoprávnený prístup k citlivým údajom
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.
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-23-199-07

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

Identifikátor

OpenSSH - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja OpenSSH vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.07.2023

CVE

CVE-2023-38408

Zasiahnuté systémy

OpenSSH vo verzii staršej ako 9.3p2

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://seclists.org/fulldisclosure/2023/Jul/31
https://exchange.xforce.ibmcloud.com/vulnerabilities/261022

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Atlassian Confluence Data Center & Server, Bamboo - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Atlassian vydala bezpečnostné aktualizácie na produkty Confluence Data Center & Server a Bamboo, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.07.2023

CVE

CVE-2023-22505, CVE-2023-22506, CVE-2023-22508

Zasiahnuté systémy

Confluence Data Center & Server 7.4.0 vo verzii staršej ako 8.2.0 alebo 7.19.8
Confluence Data Center & Server 8.0.0 vo verzii staršej ako 9.2.3 alebo 9.3.1

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.

Zdroje

https://confluence.atlassian.com/security/security-bulletin-july-18-2023-1251417643.html

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

Identifikátor

Keysight N6845A - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Keysight vydala bezpečnostnú aktualizáciu na svoj geolokačný server N6845A, ktorá opravuje tri bezpečnostné zraniteľnosti.
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

18.07.2023

CVE

CVE-2023-34394, CVE-2023-36853

Zasiahnuté systémy

N6854A Geolocation server vo verzii staršej ako 2.4.3

Následky

Eskalácia privilégií
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://www.cisa.gov/news-events/ics-advisories/icsa-23-199-02
https://www.zerodayinitiative.com/advisories/ZDI-23-976/

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

Identifikátor

Rockwell Automation Kinetix 5700 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu na svoj produkt Kinetix 5700, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených príkazov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

18.07.2023

CVE

CVE-2023-2263

Zasiahnuté systémy

Kinetix 5700 vo verzii staršej ako V13.003

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-23-199-01

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

Identifikátor

Crestron 3-Series - bezpečnostná zraniteľnosť

Popis

Spoločnosť Crestron vydala bezpečnostnú aktualizáciu firmvéru pre svoj produkt 3-Series, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených BACnet paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

18.07.2023

CVE

CVE-2023-38405

Zasiahnuté systémy

3-Series vo verzii firmvéru staršej ako 1.601.0050

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.crestron.com/release_notes/cp3n_1.8001.0187_release_notes.pdf
https://exchange.xforce.ibmcloud.com/vulnerabilities/260963

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

GE Digital CIMPLICITY - bezpečnostná zraniteľnosť

Popis

Spoločnosť GE Digital vydala bezpečnostnú aktualizáciu na svoj produkt CIMPLICITY, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov 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

18.07.2023

CVE

CVE-2023-3463

Zasiahnuté systémy

GE Digital CIMPLICITY vo všetkých verziách

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Pre aktualizáciu kontaktujte vašu lokálnu GE Digital podporu, viac informácií nájdete na odkaze:
https://digitalsupport.ge.com/s/contactsupport
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-23-199-06
https://www.redpacketsecurity.com/ge-cimplicity-buffer-overflow-cve-2023-3463/