BEZPEČNOSTNÝ BULLETIN

Týždeň 26. 07. 2023 - 01. 08. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Apache NiFi - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	CODESYS V3 framework - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Ninja Forms WP plugin - tri bezpečnostné zraniteľnosti	Vysoká	**8.8**
04.	Automation Runtime - bezpečnostná zraniteľnosť	Vysoká	**8.6**
05.	Johnson Controls IQ Wifi 6 - bezpečnostná zraniteľnosť	Vysoká	**8.3**
06.	Ubuntu Kernel - dve bezpečnostné zraniteľnosti	Vysoká	**7.8**
07.	Perimeter81 macOS Application - bezpečnostná zraniteľnosť	Vysoká	**7.8**
08.	Rockwell Automation ThinManager ThinServer	Vysoká	**7.5**
09.	ASUS RT-AX88U - dve bezpečnostné zraniteľnosti	Vysoká	**7.5**
10.	WAGO WLAN ETHERNET Gateway - bezpečnostná zraniteľnosť	Vysoká	**7.5**
11.	Apache Commons FileUpload - bezpečnostná zraniteľnosť	Vysoká	**7.5**
12.	CODESYS Development System a Scripting - bezpečnostná zraniteľnosť	Vysoká	**7.3**
13.	AO-OPC - bezpečnostná zraniteľnosť	Vysoká	**7.2**
14.	Ivanti Endpoint Manager Mobile - bezpečnostná zraniteľnosť	Vysoká	**7.2**
15.	Axis Communications AXIS A1001 - 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-1257

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

Identifikátor

Apache NiFi - bezpečnostná zraniteľnosť

Popis

Vývojári projektu Apache NiFi 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 zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.07.2023

CVE

CVE-2023-36542

Zasiahnuté systémy

Apache NiFi vo verzii staršej ako 1.23.0

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://exchange.xforce.ibmcloud.com/vulnerabilities/262053

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

Identifikátor

CODESYS V3 framework - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu CODESYS V3 framework. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zneužitia out-of-bounds zápisu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

31.07.2023

CVE

CVE-2022-47378, CVE-2022-47379, CVE-2022-47380, CVE-2022-47381, CVE-2022-47382, CVE-2022-47383, CVE-2022-47384, CVE-2022-47385, CVE-2022-47386, CVE-2022-47387, CVE-2022-47388, CVE-2022-47389, CVE-2022-47390, CVE-2022-47391, CVE-2022-47392, CVE-2022-47393

Zasiahnuté systémy

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v časti ZDROJE

Následky

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

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať.

Zdroje

https://cert.vde.com/en/advisories/VDE-2023-026/

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

Identifikátor

Ninja Forms WP plugin - tri bezpečnostné zraniteľnosti

Popis

Vývojári pluginu Ninja Forms pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód a následne získať neoprávnený prístup k citlivým údajom. Zneužitie zraniteľnosti vyžaduje interakciu používateľov.

Dátum prvého zverejnenia varovania

27.07.2023

CVE

CVE-2023-37979, CVE-2023-38386, CVE-2023-38393

Zasiahnuté systémy

Ninja Forms vo verzii staršej ako 3.6.26

Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.
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://patchstack.com/articles/multiple-high-severity-vulnerabilities-in-ninja-forms-plugin/
https://www.infosecurity-magazine.com/news/high-severity-flaws-ninja-forms/

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

Identifikátor

Automation Runtime - bezpečnostná zraniteľnosť

Popis

Spoločnosť B&R vydala bezpečnostnú aktualizáciu na svoj produkt Automation Runtime, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania veľkého množstva SYN požiadaviek spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

26.07.2023

CVE

CVE-2023-3242

Zasiahnuté systémy

Automation Runtime vo verzii staršej ako G4.93

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.br-automation.com/downloads_br_productcatalogue/assets/1689787619746-en-original-1.0.pdf

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

Identifikátor

Johnson Controls IQ Wifi 6 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Johnson Controls vydala bezpečnostnú aktualizáciu na svoj produkt IQ Wifi 6, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom brute-force útoku získať neoprávnený prístup do systému s oprávneniami používateľa.

Dátum prvého zverejnenia varovania

25.07.2023

CVE

CVE-2023-3548

Zasiahnuté systémy

Johnson Controls IQ Wifi 6 s firmvérom vo verzii staršej ako 2.0.2

Následky

Neoprávnený prístup do systému
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://www.cisa.gov/news-events/ics-advisories/icsa-23-206-04

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

Identifikátor

Ubuntu Kernel - dve bezpečnostné zraniteľnosti

Popis

Vývojári jadra operačného systému Linux Ubuntu vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvorených súborov eskalovať svoje privilégiá a následne spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.07.2023

CVE

CVE-2023-2640, CVE-2023-32629

Zasiahnuté systémy

Ubuntu 23.04 (Lunar Lobster) vo verzii staršej ako 6.2.0
Ubuntu 22.10 (Kinetic Kudu) vo verzii staršej ako 5.19.0
Ubuntu 22.04 LTS (Jammy Jellyfish) vo verzii staršej ako 5.19.0
Ubuntu 22.04 LTS (Jammy Jellyfish) vo verzii staršej ako 6.2.0
Ubuntu 22.04 LTS (Jammy Jellyfish) vo verzii staršej ako 5.15.0 (vrátane)
Ubuntu 20.04 LTS (Focal Fossa) vo verzii staršej ako 5.15.0 (vrátane)
Ubuntu 20.04 LTS (Focal Fossa) vo verzii staršej ako 5.4.0 (vrátane)
Ubuntu 18.04 LTS (Bionic Beaver) vo verzii staršej ako 5.4.0 (vrátane)

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať.

Zdroje

https://ubuntu.com/security/CVE-2023-2640
https://ubuntu.com/security/CVE-2023-32629
https://thehackernews.com/2023/07/gameoverlay-two-severe-linux.html
https://www.wiz.io/blog/ubuntu-overlayfs-vulnerability

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

Identifikátor

Perimeter81 macOS Application - bezpečnostná zraniteľnosť

Popis

Spoločnosť Perimeter81 vydala bezpečnostnú aktualizáciu na svoj Perimeter81 macOS agent, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne upravených príkazov eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

25.07.2023

CVE

CVE-2023-33298

Zasiahnuté systémy

Perimeter81 Mac agent vo verzii staršej ako 10.1.2.318

Následky

Eskalácia privilégií
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://support.perimeter81.com/docs/macos-agent-release-notes
https://www.kb.cert.org/vuls/id/653767
https://www.ns-echo.com/posts/cve_2023_33298.html
https://nvd.nist.gov/vuln/detail/CVE-2023-33298

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

Identifikátor

Rockwell Automation ThinManager ThinServer

Popis

Spoločnosť Rockwell Automation vydala bezpečnostné aktualizácie na svoj softvér ThinManager ThinServer, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom API volaní získať neoprávnený prístup k citlivým informáciám. Zneužitie zraniteľnosti vyžaduje aktivovanú funkciu API.

Dátum prvého zverejnenia varovania

25.07.2023

CVE

CVE-2023-2913

Zasiahnuté systémy

Rockwell Automation ThinManager ThinServer vo verzii staršej ako 13.0.3
Rockwell Automation ThinManager ThinServer vo verzii staršej ako 13.1.1

Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým informáciám

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.
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-23-206-02

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

Identifikátor

ASUS RT-AX88U - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť ASUS vydala bezpečnostnú aktualizáciu na svoj router RT-AX88U, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.07.2023

CVE

CVE-2023-34358, CVE-2023-34359

Zasiahnuté systémy

RT-AX88U s firmvérom vo verzii staršej ako 3.0.0.4_388_23748

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/262055
https://exchange.xforce.ibmcloud.com/vulnerabilities/262054

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

Identifikátor

WAGO WLAN ETHERNET Gateway - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu WLAN ETHERNET Gateway. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente zrealizovať MITM (Man In The Middle) útok a získať neoprávnený prístup k citlivým údajom prenášaným prostredníctvom "Bluetooth LE pairing" správ a vykonať neoprávnené zmeny v systéme

Dátum prvého zverejnenia varovania

31.07.2023

CVE

CVE-2022-25836

Zasiahnuté systémy

WAGO WLAN ETHERNET Gateway vo všetkých verziách

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Výrobca neplánuje vydať bezpečnostnú aktualizáciu a odporúča Bluetooth LE deaktivovať, kým sa nepoužíva.

Zdroje

https://cert.vde.com/en/advisories/VDE-2023-014/

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

Identifikátor

Apache Commons FileUpload - bezpečnostná zraniteľnosť

Popis

Vývojári balíka Apache Commons FileUpload vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
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

30.05.2023

CVE

CVE-2023-24998

Zasiahnuté systémy

Apache Commons FileUpload vo verzii staršej ako 1.5

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://lists.apache.org/thread/4xl4l09mhwg4vgsk7dxqogcjrobrrdoy
https://nvd.nist.gov/vuln/detail/CVE-2023-24998

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

Identifikátor

CODESYS Development System a Scripting - bezpečnostná zraniteľnosť

Popis

Spoločnosť CODESYS vydala bezpečnostné aktualizácie na produkty Development System a Scripting, ktoré opravujú bezpečnostnú zraniteľnosť.
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

28.07.2023

CVE

CVE-2023-3670

Zasiahnuté systémy

CODESYS Development System vo verzii staršej ako 3.5.17.0
CODESYS Scripting vo verzii staršej ako 4.1.0.0

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://cert.vde.com/en/advisories/VDE-2023-024/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

AO-OPC - bezpečnostná zraniteľnosť

Popis

Spoločnosť ABB vydala bezpečnostnú aktualizáciu na svoj server AO-OPC, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom podvrhnutia špeciálne vytvorených súborov eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.07.2023

CVE

CVE-2023-2685

Zasiahnuté systémy

AO-OPC vo verzii staršej ako 3.3.0

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť 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://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A4093&LanguageCode=en&DocumentPartId=&Action=Launch

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Ivanti Endpoint Manager Mobile - bezpečnostná zraniteľnosť

Popis

Spoločnosť Ivanti vydala bezpečnostnú aktualizáciu na svoj produkt Endpoint Manager Mobile (Core), 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 vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

28.07.2023

CVE

CVE-2023-35081

Zasiahnuté systémy

Ivanti Endpoint Manager Mobile (EPMM) vo verziách starších ako 11.8.1.2, 11.9.1.2 a 11.10.0.3

Následky

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

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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://forums.ivanti.com/s/article/KB-Arbitrary-File-Write-CVE-2023-35081?language=en_US
https://forums.ivanti.com/s/article/CVE-2023-35081-Arbitrary-File-Write?language=en_US
https://www.securityweek.com/second-ivanti-epmm-zero-day-vulnerability-exploited-in-targeted-attacks/

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

Identifikátor

Axis Communications AXIS A1001 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Axis Communications vydala bezpečnostnú aktualizáciu na svoj produkt AXIS A1001, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.07.2023

CVE

CVE-2023-21406

Zasiahnuté systémy

AXIS A1001 vo verzii staršej ako 1.65.5

Následky

Vykonanie škodlivého kódu a narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vykonanie škodlivého kódu 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.axis.com/ftp/pub/axis/software/PACS/A1001/1_65_5/A1001_1_65_5_release_notes.txt
https://www.cisa.gov/news-events/ics-advisories/icsa-23-206-01