BEZPEČNOSTNÝ BULLETIN

Týždeň 18. 10. 2023 - 24. 10. 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-1381

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

Identifikátor

Qnap produkty - viacero bezpečnostných zraniteľností

Popis

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

Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte Video Station, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom SQL injekcie vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.10.2023

CVE

CVE-2023-20032, CVE-2023-20052, CVE-2023-23365, CVE-2023-23366, CVE-2023-23370, CVE-2023-23371, CVE-2023-32971, CVE-2023-32972, CVE-2023-32974, CVE-2023-32976, CVE-2023-34975, CVE-2023-34976, CVE-2023-34977

Zasiahnuté systémy
Music Station vo verzii staršej ako 5.3.22 QTS 5.0.1.2376 vo verzii staršej ako build 20230421 QuTS hero h5.0.1.2376 vo verzii staršej ako build 20230421 QuTScloud vo verzii staršej ako c5.0.1.2374 QTS 5.0.1.2425 vo verzii staršej ako build 20230609 QTS 5.1.0.2444 vo verzii staršej ako build 20230629 QTS 4.5.4.2467 vo verzii staršej ako build 20230718 QuTS hero h5.0.1.2515 vo verzii staršej ako build 20230907 QuTS hero h5.1.0.2424 vo verzii staršej ako build 20230609 QuTS hero h4.5.4.2476 vo verzii staršej ako build 20230728 QuTScloud vo verzii staršej ako c5.1.0.2498 QVPN Windows vo verzii staršej ako 2.1.0.0518 QVPN Windows vo verzii staršej ako 2.2.0.0823 QTS 5.1.0.2444 vo verzii staršej ako build 20230629 QuTS hero h5.1.0.2424 vo verzii staršej ako build 20230609 QuTScloud vo verzii staršej ako c5.1.0.2498 Container Station vo verzii staršej ako 2.6.7.44 Video Station vo verzii staršej ako 5.7.0 (2023/07/27) QTS 5.1.0.2444 vo verzii staršej ako build 20230629 QTS 5.0.1.2425 vo verzii staršej ako build 20230609 QTS 4.5.4.2467 vo verzii staršej ako build 20230718 QuTS hero h5.1.0.2424 vo verzii staršej ako build 20230609 QuTS hero h5.0.1.2515 vo verzii staršej ako build 20230907 QuTS hero h4.5.4.2476 vo verzii staršej ako build 20230728 QuTScloud vo verzii staršej ako c5.1.0.2498

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.qnap.com/en/security-advisory/qsa-23-28 https://www.qnap.com/en/security-advisory/qsa-23-26 https://www.qnap.com/en/security-advisory/qsa-23-37 https://www.qnap.com/en/security-advisory/qsa-23-36 https://www.qnap.com/en/security-advisory/qsa-23-39 https://www.qnap.com/en/security-advisory/qsa-23-42 https://www.qnap.com/en/security-advisory/qsa-23-44 https://www.qnap.com/en/security-advisory/qsa-23-52 https://www.qnap.com/en/security-advisory/qsa-23-41

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

Identifikátor

MOXA TN-5900 a TN-4900 - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Moxa vydala bezpečnostné aktualizácie na web servery série TN-5900 a TN-4900, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov 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

20.10.2023

CVE

CVE-2023-33237, CVE-2023-33238, CVE-2023-33239, CVE-2023-34213, CVE-2023-34214, CVE-2023-34215, CVE-2023-34216, CVE-2023-34217

Zasiahnuté systémy

TN-5900 Series vo verzii firmvéru staršej ako v3.4
TN-4900 Series vo verzii firmvéru staršej ako v3.0
EDR-810 Series vo verzii firmvéru staršej ako v5.12.29
EDR-G902 Series vo verzii firmvéru staršej ako v5.7.21
EDR-G903 Series vo verzii firmvéru staršej ako v5.7.21
EDR-G9010 Series vo verzii firmvéru staršej ako v3.0
NAT-102 Series vo verzii firmvéru staršej ako v1.0.5

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.moxa.com/en/support/product-support/security-advisory/mpsa-230402-tn-5900-and-tn-4900-series-web-server-multiple-vulnerabilities

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

Identifikátor

QUSBCam2 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Qnap vydala bezpečnostnú aktualizáciu na svoj produkt QUSBCam2, 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

20.10.2023

CVE

CVE-2023-23373

Zasiahnuté systémy

QUSBCam2 vo verzii staršej ako 2.0.3

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.qnap.com/en/security-advisory/qsa-23-43
https://nvd.nist.gov/vuln/detail/CVE-2023-23373

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

Identifikátor

Rockwell Automation FactoryTalk Linx - bezpečnostná zraniteľnosť

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu na svoj produkt FactoryTalk Linx, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených paketov získať neoprávnený prístup k citlivým údajom a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

17.10.2023

CVE

CVE-2023-29464

Zasiahnuté systémy

FactoryTalk Linx vo verzii staršej ako v6.20 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-290-02

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

Identifikátor

Sante FFT Imaging a DICOM Viewer Pro - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Santesoft vydala bezpečnostné aktualizácie na svoje produkty Sante FFT Imaging a DICOM Viewer Pro, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov DICOM súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.10.2023

CVE

CVE-2023-35986, CVE-2023-39431, CVE-2023-5059

Zasiahnuté systémy

Sante FFT Imaging vo verzii staršej ako v1.4.1.
Sante DICOM Viewer Pro vo verzii staršej ako v12.2.6

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.

Zdroje

https://www.cisa.gov/news-events/ics-medical-advisories/icsma-23-285-02
https://www.cisa.gov/news-events/ics-medical-advisories/icsma-23-285-01

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

Identifikátor

Schneider Electric IGSS - bezpečnostná zraniteľnosť

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoj produkt Interactive Graphical SCADA System, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.10.2023

CVE

CVE-2023-4516

Zasiahnuté systémy

Update Service vo verzii staršej ako 16.0.0.23212

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.
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-23-285-16

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.7
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SonicWall SonicOS - viacero bezpečnostných zraniteľností

Popis

Spoločnosť SonicWall vydala bezpečnostné aktualizácie na svoj operačný systém SonicOS, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

17.10.2023

CVE

CVE-2023-39276, CVE-2023-39277, CVE-2023-39278, CVE-2023-39279, CVE-2023-39280, CVE-2023-41711, CVE-2023-41712, CVE-2023-41713, CVE-2023-41715

Zasiahnuté systémy
SonicOS Gen7 - TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSA2700, NSA3700 vo verzii staršej ako 7.0.1-5145 (R5175) SonicOS Gen7 - NSA4700, NSA5700, NSA6700, NSSP10700, NSSP11700, NSSP13700 vo verzii staršej ako 7.0.1-5145 (R5176) SonicOS Gen7 - NSv (VMWARE, AWS, AWS-PAYG, AZURE, HYPER-V) vo verzii staršej ako 7.0.1-5145 (R2363) SonicOS Gen7 - NSv (KVM) vo verzii staršej ako 7.0.1-5145 (R2364) SonicOS Gen7 – NSSP15700 vo verzii staršej ako 7.0.1-5145 (R1468) SonicOS Gen6 SonicOSv - NSv (10, 25, 50, 100, 200, 300, 400, 800, 1600) pre VMWare vo verzii staršej ako 6.5.4.4-44v-21-2340 SonicOS vo verzii staršej ako 6.5.4.4-44v-21-2340 SonicOS NSv (10, 25, 50, 100, 200, 300, 400, 800, 1600) pre Hyper-V vo verzii staršej ako 6.5.4.4-44v-21-2340 SonicOS vo verzii staršej ako 6.5.4.4-44v-21-2340 SonicOS NSv (10, 25, 50, 100, 200, 300, 400, 800, 1600) pre KVM vo verzii staršej ako 6.5.4.4-44v-21-2340 SonicOS vo verzii staršej ako 6.5.4.4-44v-21-2340 SonicOS NSv (200, 400, 800, 1600) pre AWS NSv (200, 400, 800, 1600) pre AWS-PAYG vo verzii staršej ako 6.5.4.4-44v-21-2340 SonicOS vo verzii staršej ako 6.5.4.4-44v-21-2340 SonicOS NSv (200, 400, 800, 1600) pre Azure vo verzii staršej ako 6.5.4.4-44v-21-2340 SonicOS Gen6 Firewalls - SOHOW, TZ 300, TZ 300W, TZ 400, TZ 400W, TZ 500, TZ 500W, TZ 600, NSA 2600, NSA 2650, vo verzii staršej ako 6.5 SonicOS vo verzii staršej ako 6.5 SonicOS NSA 3600, NSA 3650, NSA 4600, NSA 4650, NSA 5600, NSA 5650, NSA 6600, NSA 6650, SM 9200, SM 9250, vo verzii staršej ako 6.5 SonicOS vo verzii staršej ako 6.5 SonicOS SM 9400, SM 9450, SM 9600, SM 9650, TZ 300P, TZ 600P, SOHO 250, SOHO 250W, TZ 350, TZ 350W vo verzii staršej ako 6.5

Následky
Zneprístupnenie služby

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012 https://exchange.xforce.ibmcloud.com/vulnerabilities/268839

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

Identifikátor

Hikvision Access Control a Intercom produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Hikvision vydala bezpečnostné aktualizácie na svoje produkty Access Control a Intercom, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia 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

12.10.2023

CVE

CVE-2023-28809, CVE-2023-28810

Zasiahnuté systémy

DS-K1T804AXX vo verzii staršej ako V1.4.0_build221212 (vrátane)
DS-K1T341AXX vo verzii staršej ako V3.2.30_build221223 (vrátane)
DS-K1T671XXX vo verzii staršej ako V3.2.30_build221223 (vrátane)
DS-K1T343XXX vo verzii staršej ako V3.14.0_build230117 (vrátane)
DS-K1T341C vo verzii staršej ako V3.3.8_build230112 (vrátane)
DS-K1T320XXX vo verzii staršej ako V3.5.0_build220706 (vrátane)
DS-KH63 Series vo verzii staršej ako V2.2.8_build230219 (vrátane)
DS-KH85 Series vo verzii staršej ako V2.2.8_build230219 (vrátane)
DS-KH62 Series vo verzii staršej ako V1.4.62_build220414 (vrátane)
DS-KH9310-WTE1(B) vo verzii staršej ako V2.1.76_build230204 (vrátane)
DS-KH9510-WTE1(B) vo verzii staršej ako V2.1.76_build230204 (vrátane)

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.
Zasiahnuté systémy odporúčame neponechávať otvorené do verejného 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-23-285-14

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

Identifikátor

Milesight routre - bezpečnostná zraniteľnosť

Popis

Spoločnosť Milesight vydala bezpečnostnú aktualizáciu na svoje portfólio routerov, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

01.10.2023

CVE

CVE-2023-43261

Zasiahnuté systémy

Milesight UR5X, UR32L, UR32, UR35 a UR41 vo verzii firmvéru staršej ako v35.3.0.7

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do 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/win3zz/CVE-2023-43261
https://medium.com/@win3zz/inside-the-router-how-i-accessed-industrial-routers-and-reported-the-flaws-29c34213dfdf
https://nvd.nist.gov/vuln/detail/CVE-2023-43261
https://vulmon.com/searchpage?q=CVE-2023-43261

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

Identifikátor

Sophos Firewall - bezpečnostná zraniteľnosť

Popis

Spoločnosť Sophos vydala bezpečnostnú aktualizáciu na svoj produkt Sophos Firewall, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

17.10.2023

CVE

CVE-2023-5552

Zasiahnuté systémy

Sophos Firewall vo verzii staršej ako v20.0 EAP1
Sophos Firewall vo verzii staršej ako v19.5 MR1-1, MR1 a GA
Sophos Firewall vo verzii staršej ako v19.0 MR3, MR2, MR1-1 a MR1
Sophos Firewall vo verzii staršej ako v19.5 MR4 (19.5.4) a v20.0 GA

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.sophos.com/en-us/security-advisories/sophos-sa-20231017-spx-password
https://exchange.xforce.ibmcloud.com/vulnerabilities/268964

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

Identifikátor

Aruba AirWave Management Platform - bezpečnostná zraniteľnosť

Popis

Spoločnosť Aruba vydala bezpečnostnú aktualizáciu na svoj produkt AirWave Management Platform, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

18.10.2023

CVE

CVE-2023-4896

Zasiahnuté systémy

HPE Aruba Networking AirWave Management Platform vo verzii staršej ako 8.3.0.2

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://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04546en_us

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Advantech WebAccess - bezpečnostná zraniteľnosť

Popis

Spoločnosť Advantech vydala bezpečnostnú aktualizáciu na svoj produkt WebAccess, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

12.10.2023

CVE

CVE-2023-4215

Zasiahnuté systémy

WebAccess vo verzii staršej ako 9.1.4.

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-23-285-15

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Cisco Catalyst SD-WAN Manager - bezpečnostná zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt Catalyst SD-WAN Manager, 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 získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

18.10.2023

CVE

CVE-2023-20261

Zasiahnuté systémy

Cisco Catalyst SD-WAN Manager vo verzii staršej ako 20.6.6
Bezpečnostné záplaty pre Catalyst SD-WAN Manager vo verzii 20.7 a vyšších sú v príprave

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe