BEZPEČNOSTNÝ BULLETIN

Týždeň 31. 05. 2023 - 06. 06. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Sonos One Speaker - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	Google Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Contec CONPROSYS HMI - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	Splunk - tri bezpečnostné zraniteľnosti	Vysoká	**8.8**
05.	Samsung Galaxy Store - tri bezpečnostné zraniteľnosti	Vysoká	**8.8**
06.	Google Android - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
07.	IBM Aspera Connect a Aspera Cargo - dve bezpečnostné zraniteľnosti	Vysoká	**8.4**
08.	KylinSoft KylinOS - tri bezpečnostné zraniteľnosti	Vysoká	**8.4**
09.	Delta Electronics CNCSoft-B DOPSoft - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
10.	Apache Cassandra - bezpečnostná zraniteľnosť	Vysoká	**7.8**
11.	ASPECT® Control Engines (ACE) - dve bezpečnostné zraniteľnosti	Vysoká	**7.8**
12.	FUJI ELECTRIC FRENIC RHC Loader - tri bezpečnostné zraniteľnosti	Vysoká	**7.8**
13.	Wireshark - bezpečnostná zraniteľnosť	Vysoká	**7.5**
14.	Microsoft Edge - dve bezpečnostné zraniteľnosti	Vysoká	**7.5**
15.	Advantech WebAccess/SCADA - bezpečnostná zraniteľnosť	Vysoká	**7.3**
16.	OpenSSL - bezpečnostná zraniteľnosť	Stredná	**6.5**

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-1171

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

Identifikátor

Sonos One Speaker - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Sonos vydala bezpečnostnú aktualizáciu na svoj produkt One Speaker, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.04.2023

CVE

CVE-2023-20869, CVE-2023-27352, CVE-2023-27353, CVE-2023-27354, CVE-2023-27355, CVE-2023-27533

Zasiahnuté systémy

Sonos S2 app vo verzii staršej ako 15.1
Sonos S1 app vo verzii staršej ako 11.7.1

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://nvd.nist.gov/vuln/detail/CVE-2023-27352
https://www.zerodayinitiative.com/blog/2023/5/24/exploiting-the-sonos-one-speaker-three-different-ways-a-pwn2own-toronto-highlight

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

Identifikátor

Google Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj webový prehliadač Google Chrome, ktorá opravuje 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

01.06.2023

CVE

CVE-2023-2458, CVE-2023-2929, CVE-2023-2930, CVE-2023-2931, CVE-2023-2932, CVE-2023-2933, CVE-2023-2934, CVE-2023-2935, CVE-2023-2936, CVE-2023-2937, CVE-2023-2938, CVE-2023-2939, CVE-2023-2940, CVE-2023-2941

Zasiahnuté systémy

Chrome pre Android vo verzii staršej ako 114.0.5735.57/.58
Chrome pre Windows vo verzii staršej ako 114.0.5735.90/.91
Chrome pre Mac & Linux vo verzii staršej ako 114.0.5735.90

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://exchange.xforce.ibmcloud.com/vulnerabilities/256525
https://chromereleases.googleblog.com/

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

Identifikátor

Contec CONPROSYS HMI - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Contec vydala bezpečnostnú aktualizáciu na svoj produkt CONPROSYS HMI, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

31.05.2023

CVE

CVE-2023-2758, CVE-2023-28399, CVE-2023-28651, CVE-2023-28657, CVE-2023-28713, CVE-2023-28824, CVE-2023-29154

Zasiahnuté systémy

CONPROSYS HMI System (CHS) vo verzii staršej ako 3.5.3

Následky

Eskalácia privilégií
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

http://jvn.jp/en/vu/JVNVU93372935/index.html

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

Identifikátor

Splunk - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Splunk vydala bezpečnostné aktualizácie na svoje produkty Splunk Enterprise a Splunk Cloud Platform, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

01.06.2023

CVE

CVE-2023-32706, CVE-2023-32707, CVE-2023-32708

Zasiahnuté systémy

Splunk Enterprise 8.1 vo verzii staršej ako 8.1.14
Splunk Enterprise 8.2 vo verzii staršej ako 8.2.11
Splunk Enterprise 9.0 vo verzii staršej ako 9.0.5
Splunk Cloud Platform vo verzii staršej ako 9.0.2303.100

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://advisory.splunk.com/advisories/SVD-2023-0602
https://www.securityweek.com/high-severity-vulnerabilities-patched-in-splunk-enterprise/

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

Identifikátor

Samsung Galaxy Store - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Samsung vydala bezpečnostnú aktualizáciu na svoj produkt Galaxy Store, ktorá opravuje tri bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov alebo webstránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

31.05.2023

CVE

CVE-2023-21514, CVE-2023-21515, CVE-2023-21516

Zasiahnuté systémy

Galaxy Store staršie ako 4.5.49.8

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://nvd.nist.gov/vuln/detail/CVE-2023-21515
https://www.zerodayinitiative.com/advisories/ZDI-23-774/
https://www.zerodayinitiative.com/advisories/ZDI-23-773/
https://www.zerodayinitiative.com/advisories/ZDI-23-772/

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

Identifikátor

Google Android - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj operačný systém Android, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.06.2023

CVE

CVE-2021-0701, CVE-2021-0945, CVE-2022-22060, CVE-2022-22706, CVE-2022-28349, CVE-2022-33251, CVE-2022-33257, CVE-2022-33264, CVE-2022-33292, CVE-2022-40516, CVE-2022-40517, CVE-2022-40520, CVE-2022-40521, CVE-2022-40523, CVE-2022-40529, CVE-2022-40533, CVE-2022-40536, CVE-2022-40538, CVE-2022-46781, CVE-2022-48390, CVE-2022-48391, CVE-2022-48392, CVE-2022-48438, CVE-2023-21095, CVE-2023-21101, CVE-2023-21105, CVE-2023-21108, CVE-2023-21115, CVE-2023-21120, CVE-2023-21121, CVE-2023-21122, CVE-2023-21123, CVE-2023-21124, CVE-2023-21126, CVE-2023-21127, CVE-2023-21128, CVE-2023-21129, CVE-2023-21130, CVE-2023-21131, CVE-2023-21135, CVE-2023-21136, CVE-2023-21137, CVE-2023-21138, CVE-2023-21139, CVE-2023-21141, CVE-2023-21142, CVE-2023-21143, CVE-2023-21144, CVE-2023-21628, CVE-2023-21656, CVE-2023-21657, CVE-2023-21658, CVE-2023-21659, CVE-2023-21661, CVE-2023-21669, CVE-2023-21670

Zasiahnuté systémy

Android vo verzii pred úrovňou aktualizácií 2023-06-05

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://source.android.com/docs/security/bulletin/2023-06-01
https://www.cybersecurity-help.cz/vdb/SB2023060622

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

IBM Aspera Connect a Aspera Cargo - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie na produkty Aspera Connect a Aspera Cargo, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.06.2023

CVE

CVE-2023-22862, CVE-2023-27285

Zasiahnuté systémy

IBM Aspera Connect pre Linux vo verzii staršej ako 4.2.6
IBM Aspera Connect pre Mac OSX vo verzii staršej ako 4.2.6
IBM Aspera Connect pre Windows vo verzii staršej ako 4.2.6
IBM Aspera Cargo pre Linux vo verzii staršej ako 4.2.6
IBM Aspera Cargo pre Mac OSX vo verzii staršej ako 4.2.6
IBM Aspera Cargo pre Windows vo verzii staršej ako 4.2.6

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.ibm.com/support/pages/node/7001053
https://exchange.xforce.ibmcloud.com/vulnerabilities/248625

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.4
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

KylinSoft KylinOS - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť KylinSoft vydala bezpečnostnú aktualizáciu na svoj operačný systém KylinOS, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať neoprávnené zmeny v systéme a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

05.06.2023

CVE

CVE-2023-3096, CVE-2023-3098, CVE-2023-3099

Zasiahnuté systémy

KylinOS youker-assistant vo verzii staršej ako 3.0.2-0kylin6k70-23

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/257111
https://github.com/i900008/vulndb/blob/main/kylinos_vul4.md

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

Identifikátor

Delta Electronics CNCSoft-B DOPSoft - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na svoj produkt CNCSoft-B DOPSoft, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky alebo súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.06.2023

CVE

-

Zasiahnuté systémy

CNCSoft-B DOPSoft vo verzii staršej ako v4.0.0.82

Následky

Vykonanie škodlivého kódu a 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 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.zerodayinitiative.com/advisories/ZDI-23-781/
https://www.zerodayinitiative.com/advisories/ZDI-23-782/
https://www.zerodayinitiative.com/advisories/ZDI-23-783/
https://www.zerodayinitiative.com/advisories/ZDI-23-784/
https://www.zerodayinitiative.com/advisories/ZDI-23-785/
https://www.zerodayinitiative.com/advisories/ZDI-23-786/
https://www.zerodayinitiative.com/advisories/ZDI-23-787/
https://www.zerodayinitiative.com/advisories/ZDI-23-788/
https://www.zerodayinitiative.com/advisories/ZDI-23-789/
https://www.zerodayinitiative.com/advisories/ZDI-23-790/
https://www.zerodayinitiative.com/advisories/ZDI-23-791/
https://www.zerodayinitiative.com/advisories/ZDI-23-792/
https://www.zerodayinitiative.com/advisories/ZDI-23-793/
https://www.zerodayinitiative.com/advisories/ZDI-23-794/
https://www.zerodayinitiative.com/advisories/ZDI-23-795/
https://www.zerodayinitiative.com/advisories/ZDI-23-796/
https://www.zerodayinitiative.com/advisories/ZDI-23-797/
https://www.zerodayinitiative.com/advisories/ZDI-23-798/
https://www.zerodayinitiative.com/advisories/ZDI-23-799/
https://www.zerodayinitiative.com/advisories/ZDI-23-800/
https://www.zerodayinitiative.com/advisories/ZDI-23-801/
https://www.zerodayinitiative.com/advisories/ZDI-23-802/
https://www.zerodayinitiative.com/advisories/ZDI-23-803/
https://www.zerodayinitiative.com/advisories/ZDI-23-804/
https://www.zerodayinitiative.com/advisories/ZDI-23-805/
https://www.zerodayinitiative.com/advisories/ZDI-23-806/
https://www.zerodayinitiative.com/advisories/ZDI-23-807/
https://www.zerodayinitiative.com/advisories/ZDI-23-808/
https://www.zerodayinitiative.com/advisories/ZDI-23-809/
https://www.zerodayinitiative.com/advisories/ZDI-23-810/
https://www.zerodayinitiative.com/advisories/ZDI-23-811/
https://www.zerodayinitiative.com/advisories/ZDI-23-812/
https://www.zerodayinitiative.com/advisories/ZDI-23-813/
https://www.zerodayinitiative.com/advisories/ZDI-23-814/
https://www.zerodayinitiative.com/advisories/ZDI-23-815/
https://www.zerodayinitiative.com/advisories/ZDI-23-816/
https://www.zerodayinitiative.com/advisories/ZDI-23-817/

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

Identifikátor

Apache Cassandra - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja Apache Cassandra vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injekcie špeciálne upravených príkazov eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.05.2023

CVE

CVE-2023-30601

Zasiahnuté systémy

Apache Cassandra vo verzii staršej ako 4.0.10 a 4.1.2

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/oss-sec/2023/q2/201
https://exchange.xforce.ibmcloud.com/vulnerabilities/256502

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

Identifikátor

ASPECT® Control Engines (ACE) - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť ABB vydala bezpečnostné aktualizácie na produkty sérií ASPECT, NEXUS a MATRIX, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepristupnenie služby.

Dátum prvého zverejnenia varovania

01.06.2023

CVE

CVE-2023-0635, CVE-2023-0636

Zasiahnuté systémy

ASPECT®-Enterprise ASP-ENT-x vo verzii firmvéru staršej ako 3.07.01
NEXUS Series NEX-2x,NEXUS-3-x vo verzii firmvéru staršej ako 3.07.01
MATRIX Series MAT-x vo verzii firmvéru staršej ako 3.07.01

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://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.244777221.1288793204.1685942765-623691999.1681733553

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

Identifikátor

FUJI ELECTRIC FRENIC RHC Loader - tri bezpečnostné zraniteľnosti

Popis

Vývojári nástroja FUJI ELECTRIC FRENIC RHC Loader vydali bezpečnostnú aktualizáciu svojho produktu, ktorá odstraňuje 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

02.06.2023

CVE

CVE-2023-29160, CVE-2023-29167, CVE-2023-29498

Zasiahnuté systémy

FRENIC RHC Loader vo verzii staršej ako v1.3.0.1

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

http://jvn.jp/en/vu/JVNVU97809354/index.html

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

Identifikátor

Wireshark - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja Wireshark vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom injekcie špeciálne vytvorených paketov do analyzovanej sieťovej prevádzky alebo PCAP súborov spôsobiť zneprístupnenie služby.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

30.05.2023

CVE

CVE-2023-2879

Zasiahnuté systémy

Wireshark vo verzii staršej ako 3.6.14 a 4.0.6

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2879.json
https://gitlab.com/wireshark/wireshark/-/issues/19068
https://nvd.nist.gov/vuln/detail/CVE-2023-2879

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

Identifikátor

Microsoft Edge - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoj prehliadač Edge, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

02.06.2023

CVE

CVE-2023-29345, CVE-2023-33143

Zasiahnuté systémy

Microsoft Edge vo verzii staršej ako 114.0.1823.37

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33143
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29345

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

Identifikátor

Advantech WebAccess/SCADA - bezpečnostná zraniteľnosť

Popis

Spoločnosť Advantech vydala bezpečnostnú aktualizáciu na svoj produkt WebAccess/SCADA, ktorá opravuje 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

30.05.2023

CVE

CVE-2023-2866

Zasiahnuté systémy

WebAccess/SCADA vo verzii staršej ako V9.1.4

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.
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://exchange.xforce.ibmcloud.com/vulnerabilities/256514
https://www.cisa.gov/news-events/ics-advisories/icsa-23-150-01

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

Identifikátor

OpenSSL - bezpečnostná zraniteľnosť

Popis

Vývojári projektu OpenSSL vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom špeciálne vytvorených ASN.1 objektov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

30.05.2023

CVE

CVE-2023-2650

Zasiahnuté systémy

OpenSSL 3.0 vo verzii staršej ako 3.0.9
OpenSSL 3.1 vo verzii staršej ako 3.1.1
OpenSSL 1.1.1 vo verzii staršej ako 1.1.1u
OpenSSL 1.0.2 vo verzii staršej ako 1.0.2zh (len premium support zákazníci)

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.openssl.org/news/secadv/20230530.txt
https://www.securitynewspaper.com/2023/05/30/openssl-flaw-allows-slowing-down-websites-and-applications-with-client-authentication/
https://www.suse.com/security/cve/CVE-2023-2650.html