BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 09. 2023 - 12. 09. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Schweizer Engineering Laboratories produkty - kritická bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	AC500 V3 - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Google Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	Apple produkty - tri bezpečnostné zraniteľnosti	Vysoká	**8.8**
05.	Festo MSE6-C2M/D2M/E2M - bezpečnostná zraniteľnosť	Vysoká	**8.8**
06.	D-Link DIR-1325 - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
07.	QNAP QuLog Center (QTS, QuTS hero a QuTScloud) - bezpečnostná zraniteľnosť	Vysoká	**8.8**
08.	Open Automation Software - viacero bezpečnostných zraniteľností	Vysoká	**8.1**
09.	NVIDIA BlueField a Cumulus Linux - tri bezpečnostné zraniteľnosti	Vysoká	**7.8**
10.	PDF-XChange Editor/Tools - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
11.	Kofax Power PDF Advanced - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
12.	Delta Electronics CNCSoft-B DPA - bezpečnostná zraniteľnosť	Vysoká	**7.8**
13.	Contec SolarView Compact - bezpečnostná zraniteľnosť	Vysoká	**7.5**
14.	Synology Router Manager - viacero bezpečnostných zraniteľností	Vysoká	**7.2**
15.	Apache Superset - tri bezpečnostné zraniteľnosti	Stredná	**6.6**
16.	Real-time Video Transmission Gear séria IP - bezpečnostná zraniteľnosť	Stredná	**5.9**

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-1317

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

Identifikátor

Schweizer Engineering Laboratories produkty - kritická bezpečnostná zraniteľnosť

Popis

Spoločnosť Schweizer Engineering Laboratories vydala bezpečnostné aktualizácie na produkty QuickSet a Grid Configurator, ktoré opravujú viacero bezpečnostných zraniteľností.
Kritická bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

31.08.2023

CVE

CVE-2023-31168, CVE-2023-31169, CVE-2023-31170, CVE-2023-31171, CVE-2023-31172, CVE-2023-31173, CVE-2023-31174, CVE-2023-31175, CVE-2023-34392

Zasiahnuté systémy

SEL-5037 SEL Grid Configurator vo verzii staršej ako 4.5.0.20
QuickSet vo verzii staršej ako 7.1.4.0

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne 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.nozominetworks.com/blog/9-new-vulnerabilities-impact-schweitzer-engineering-labs-software
https://selinc.com/products/software/latest-software-versions/

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

Identifikátor

AC500 V3 - viacero bezpečnostných zraniteľností

Popis

Spoločnosť ABB vydala bezpečnostnú aktualizáciu na svoje portfólio produktov AC500 V3, ktorá opravuje 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 alebo vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.09.2023

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-2022-47392, CVE-2022-47393

Zasiahnuté systémy

AC500 V3 produkty (PM5xxx) vo verzii firmvéru staršej ako 3.7.0

Následky

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://search.abb.com/library/Download.aspx?DocumentID=3ADR011211&LanguageCode=en&DocumentPartId=&Action=Launch

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 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

05.09.2023

CVE

CVE-2023-4761, CVE-2023-4762, CVE-2023-4763, CVE-2023-4764

Zasiahnuté systémy

Chrome pre Mac a Linux vo verzii staršej ako 116.0.5845.179
Chrome pre Windows vo verzii staršej ako 116.0.5845.179/.180

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/2023/09/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

Apple produkty - tri bezpečnostné zraniteľnosti

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 vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.09.2023

CVE

CVE-2023-38606, CVE-2023-41061, CVE-2023-41064

Zasiahnuté systémy

iOS vo verzii staršej ako 16.6.1
iPadOS vo verzii staršej ako 16.6.1
macOS Ventura vo verzii staršej ako 13.5.2
watchOS vo verzii staršej ako 9.6.2

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

Zdroje

https://support.apple.com/en-us/HT213907
https://support.apple.com/en-us/HT213906
https://support.apple.com/en-us/HT213905
https://thehackernews.com/2023/09/apple-rushes-to-patch-zero-day-flaws.html

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

Identifikátor

Festo MSE6-C2M/D2M/E2M - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Festo MSE6.
Bezpečnostná zraniteľnosť spočíva v existencii nezdokumentovaného špeciálneho testovacieho režimu, ktorého použitie umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.09.2023

CVE

CVE-2023-3634

Zasiahnuté systémy

MSE6-C2M-5000-FB36-D-M-RG-BAR-M12L4-AGD vo všetkých verziách
MSE6-C2M-5000-FB36-D-M-RG-BAR-M12L5-AGD vo všetkých verziách
MSE6-C2M-5000-FB43-D-M-RG-BAR-M12L4-MQ1-AGD vo všetkých verziách
MSE6-C2M-5000-FB43-D-M-RG-BAR-M12L5-MQ1-AGD vo všetkých verziách
MSE6-C2M-5000-FB44-D-M-RG-BAR-AMI-AGD vo všetkých verziách
MSE6-C2M-5000-FB44-D-RG-BAR-AMI-AGD vo všetkých verziách
MSE6-D2M-5000-CBUS-S-RG-BAR- VCB-AGD vo všetkých verziách
MSE6-E2M-5000-FB13-AGD vo všetkých verziách
MSE6-E2M-5000-FB36-AGD vo všetkých verziách
MSE6-E2M-5000-FB37-AGD vo všetkých verziách
MSE6-E2M-5000-FB43-AGD vo všetkých verziách
MSE6-E2M-5000-FB44-AGD vo všetkých verziách

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní novej dokumentácie k testovaciemu režimu prísne dodržiavať odporúčané postupy.
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://cert.vde.com/en/advisories/VDE-2023-020/

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

Identifikátor

D-Link DIR-1325 - viacero bezpečnostných zraniteľností

Popis

Spoločnosť D-Link vydala bezpečnostnú aktualizáciu na svoj router DIR-1325, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.09.2023

CVE

CVE-2023-41186, CVE-2023-41187, CVE-2023-41188, CVE-2023-41189, CVE-2023-41190, CVE-2023-41191, CVE-2023-41192, CVE-2023-41193, CVE-2023-41194, CVE-2023-41195, CVE-2023-41196, CVE-2023-41197, CVE-2023-41198, CVE-2023-41199, CVE-2023-41200, CVE-2023-41201, CVE-2023-41202, CVE-2023-41203, CVE-2023-41204, CVE-2023-41205, CVE-2023-41206, CVE-2023-41207, CVE-2023-41208, CVE-2023-41209, CVE-2023-41210, CVE-2023-41211, CVE-2023-41212, CVE-2023-41213, CVE-2023-41214, CVE-2023-41216, CVE-2023-41217, CVE-2023-41218, CVE-2023-41219, CVE-2023-41220, CVE-2023-41221, CVE-2023-41222, CVE-2023-41223, CVE-2023-41224, CVE-2023-41225, CVE-2023-41226, CVE-2023-41227, CVE-2023-41228, CVE-2023-41229, CVE-2023-41230

Zasiahnuté systémy

DAP-1325 vo verzii firmvéru staršej ako v1.09b03 Beta-Hotfix

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://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10351
https://www.zerodayinitiative.com/advisories/ZDI-23-1295/

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

Identifikátor

QNAP QuLog Center (QTS, QuTS hero a QuTScloud) - bezpečnostná zraniteľnosť

Popis

Spoločnosť Qnap vydala bezpečnostnú aktualizáciu na svoj produkt QuLog Center, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

08.09.2023

CVE

CVE-2023-23354

Zasiahnuté systémy

QTS 5.0.1: QuLog Center vo verzii staršej ako 1.5.0.738 (2023/03/06)
QTS 4.5.4: QuLog Center vo verzii staršej ako 1.3.1.645 (2023/02/22)
QuTS Hero h5.0.1: QuLog Center vo verzii staršej ako 1.5.0.738 (2023/03/06)
QuTS hero h4.5.4: QuLog Center vo verzii staršej ako 1.3.1.645 (2023/02/22)
QuTscloud c5.0.1: QuLog Center vo verzii staršej ako 1.4.1.691 (2023/03/01)

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-23-13

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

Identifikátor

Open Automation Software - viacero bezpečnostných zraniteľností

Popis

Vývojári platformy Open Automation Software vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup do systému a následne spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.09.2023

CVE

CVE-2023-31242, CVE-2023-32271, CVE-2023-32615, CVE-2023-34317, CVE-2023-34353, CVE-2023-34994, CVE-2023-34998, CVE-2023-35124

Zasiahnuté systémy

OAS Platform vo verzii staršej ako 9.00.0006

Následky

Neoprávnený prístup do systému
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://exchange.xforce.ibmcloud.com/vulnerabilities/265173
https://talosintelligence.com/vulnerability_reports/TALOS-2023-1769
https://talosintelligence.com/vulnerability_reports/TALOS-2023-1770
https://talosintelligence.com/vulnerability_reports/TALOS-2023-1771
https://talosintelligence.com/vulnerability_reports/TALOS-2023-1772
https://talosintelligence.com/vulnerability_reports/TALOS-2023-1773
https://talosintelligence.com/vulnerability_reports/TALOS-2023-1774
https://talosintelligence.com/vulnerability_reports/TALOS-2023-1775
https://talosintelligence.com/vulnerability_reports/TALOS-2023-1776

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

Identifikátor

NVIDIA BlueField a Cumulus Linux - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie na produkty Cumulus Linux a NVIDIA BlueField Data Processing Unit, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť nachádzajúca sa v produkte BlueField spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.09.2023

CVE

CVE-2023-25519, CVE-2023-25525, CVE-2023-25526

Zasiahnuté systémy

BlueField 1 vo všetkých verziách
BlueField 2 LTS vo verzii firmvéru staršej ako 24.35.3006 a verzii BFB staršej ako 3.9.5
BlueField 2 GA vo verzii firmvéru staršej ako 24.38.1002 a verzii BFB staršej ako 4.2.0
BlueField 3 GA vo verzii firmvéru staršej ako 32.38.1002 a verzii BFB staršej ako 4.2.0
Cumulus Linux vo verzii staršej ako 5.6.0 a 5.5.0

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému
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://nvidia.custhelp.com/app/answers/detail/a_id/5480
https://nvidia.custhelp.com/app/answers/detail/a_id/5479

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

Identifikátor

PDF-XChange Editor/Tools - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Tracker Software vydala bezpečnostné aktualizácie na svoje produkty PDF-XChange Editor/Tools a Pro, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.09.2023

CVE

CVE-2022-37351, CVE-2023-39483, CVE-2023-39484, CVE-2023-39485, CVE-2023-39486, CVE-2023-42045, CVE-2023-42046, CVE-2023-42047, CVE-2023-42048, CVE-2023-42071, CVE-2023-42072, CVE-2023-42075, CVE-2023-42076, CVE-2023-42077, CVE-2023-42078, CVE-2023-42079, CVE-2023-42080, CVE-2023-42081, CVE-2023-42082, CVE-2023-42083, CVE-2023-42084, CVE-2023-42085, CVE-2023-42086, CVE-2023-42087, CVE-2023-42088

Zasiahnuté systémy

PDF-XChange Editor vo verzii staršej ako 10.1.0.380
PDF-Tools vo verzii staršej ako 10.1.0.380
PDF-XChange PRO vo verzii staršej ako 10.1.0.380

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://www.tracker-software.com/support/security-bulletins.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/265633

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

Identifikátor

Kofax Power PDF Advanced - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Kofax vydala bezpečnostnú aktualizáciu na svoj produkt Kofax Power PDF Advanced, ktorá opravuje 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

08.09.2023

CVE

CVE-2023-42036, CVE-2023-42037, CVE-2023-42038, CVE-2023-42039

Zasiahnuté systémy

Kofax Power PDF Advanced vo verzii staršej ako 5.0.0.12

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://www.zerodayinitiative.com/advisories/ZDI-23-1395/
https://docshield.kofax.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.12.htm

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

Identifikátor

Delta Electronics CNCSoft-B DPA - bezpečnostná zraniteľnosť

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na svoj produkt CNCSoft-B DPA, ktorá opravuje bezpečnostnú zraniteľnosť.
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

08.09.2023

CVE

CVE-2023-4685

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.
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.

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-23-1400/
https://www.cisa.gov/news-events/ics-advisories/icsa-23-157-01

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

Identifikátor

Contec SolarView Compact - bezpečnostná zraniteľnosť

Popis

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

Dátum prvého zverejnenia varovania

08.09.2023

CVE

CVE-2023-40924

Zasiahnuté systémy

SolarView Compact vo verzii staršej ako 6.00

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://exchange.xforce.ibmcloud.com/vulnerabilities/265698

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

Identifikátor

Synology Router Manager - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Synology vydala bezpečnostnú aktualizáciu na svoj produkt Synology Router Manager, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

31.08.2023

CVE

CVE-2023-41738, CVE-2023-41739, CVE-2023-41740, CVE-2023-41741

Zasiahnuté systémy

Synology Router Manager vo verzii staršej ako 1.3.1-9346-6

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.synology.com/en-global/security/advisory/Synology_SA_23_10

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

Identifikátor

Apache Superset - tri bezpečnostné zraniteľnosti

Popis

Vývojári platformy Apache Superset vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom podvrhnutia špeciálne vytvoreného Python objektu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.09.2023

CVE

CVE-2023-30776, CVE-2023-37941, CVE-2023-39265

Zasiahnuté systémy

Apache Superset vo verzii staršej ako 2.1.1

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-2023-37941
https://nvd.nist.gov/vuln/detail/CVE-2023-39265
https://nvd.nist.gov/vuln/detail/CVE-2023-30776
https://www.horizon3.ai/apache-superset-part-ii-rce-credential-harvesting-and-more/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.9
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Real-time Video Transmission Gear séria IP - bezpečnostná zraniteľnosť

Popis

Spoločnosť Fujitsu vydala bezpečnostnú aktualizáciu na svoje portfólio produktov Real-time Video Transmission Gear "IP series", ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému a následne neoprávnený prístup k citlivým údajom alebo spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

05.09.2023

CVE

CVE-2023-38433

Zasiahnuté systémy

Real-time Video Transmission Gear "IP series" IP-HE950E vo verziách firmvéru V01L001 až V01L053
Real-time Video Transmission Gear "IP series" IP-HE950D vo verziách firmvéru V01L001 až V01L053
Real-time Video Transmission Gear "IP series" IP-HE900E vo verziách firmvéru V01L001 až V01L010
Real-time Video Transmission Gear "IP series" IP-HE900D vo verziách firmvéru V01L001 až V01L004
Real-time Video Transmission Gear "IP series" IP-900E / IP-920E vo verziách firmvéru V01L001 až V02L061
Real-time Video Transmission Gear "IP series" IP-900D / IP-900□D / IP-920D vo verziách firmvéru V01L001to V02L061
Real-time Video Transmission Gear "IP series" IP-90 vo verziách firmvéru V01L001 až V01L013
Real-time Video Transmission Gear "IP series" IP-9610 vo verziách firmvéru V01L001 až V02L007

Následky

Neoprávnený prístup do systému
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-23-248-01