BEZPEČNOSTNÝ BULLETIN

Týždeň 13. 12. 2023 - 19. 12. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Extreme Networks HiveOS a AP410C - dve bezpečnostné zraniteľnosti	Vysoká	**8.8**
02.	Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Palo Alto Networks PAN-OS - bezpečnostná zraniteľnosť	Vysoká	**8.8**
04.	pfSense - tri bezpečnostné zraniteľnosti	Vysoká	**8.8**
05.	HPE Cray Programming Environment Slurm - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
06.	Apache Dubbo - bezpečnostná zraniteľnosť	Vysoká	**8.8**
07.	Dell PowerProtect DD - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
08.	X.Org X server - dve bezpečnostné zraniteľnosti	Vysoká	**8.4**
09.	Fortinet produkty - tri bezpečnostné zraniteľnosti	Vysoká	**8.3**
10.	Parallels Desktop - tri bezpečnostné zraniteľnosti	Vysoká	**8.3**
11.	FXC AE1021PE a AE1021 - bezpečnostná zraniteľnosť	Vysoká	**8.0**
12.	Check Point Harmony Endpoint/ZoneAlarm Extreme Security - bezpečnostná zraniteľnosť	Vysoká	**7.8**
13.	Adobe produkty - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
14.	Intel Driver & Support Assistant - zero day bezpečnostná zraniteľnosť	Vysoká	**7.8**
15.	Cambium ePMP 5GHz Force 300-25 - bezpečnostná zraniteľnosť	Vysoká	**7.8**
16.	Ivanti Avalanche - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
17.	Progress Software WhatsUp Gold - viacero bezpečnostných zraniteľností	Vysoká	**7.6**
18.	Bosch produkty - tri bezpečnostné zraniteľnosti	Vysoká	**7.5**
19.	Johnson Controls Kantech Gen1 ioSmart - bezpečnostná zraniteľnosť	Vysoká	**7.5**
20.	Zoom produkty - viacero bezpečnostných zraniteľností	Vysoká	**7.3**
21.	PaperCut MF a NG - dve bezpečnostné zraniteľnosti	Vysoká	**7.0**
22.	OpenAI ChatGPT - zero day 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-1447

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

Identifikátor

Extreme Networks HiveOS a AP410C - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Extreme Networks vydala bezpečnostné aktualizácie na produkty HiveOS a AP410C, ktoré opravujú dve bezpečnostné zraniteľnosti.
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

12.12.2023

CVE

CVE-2023-46271, CVE-2023-46272

Zasiahnuté systémy

IQ Engine (HiveOS) pre AP30, AP122, AP122X, AP130, AP150W, AP230,□ AP245X, AP250,□AP550, AP1130 vo verzii staršej ako 10.6r1a
IQ Engine (HiveOS) pre AP302W, AP305C/CX, AP305C-1, AP410C, AP410C-1, AP460C, AP460S6C, AP460S12C, AP510C/CX, AP630, AP650, AP650X, AP3000,A3000X,AP4000, AP4000-1, AP5010, AP5050D, AP5050U vo verzii staršej ako 10.6r5

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://extreme-networks.my.site.com/ExtrArticleDetail?an=000115355&q=CVE-2023-46272
https://www.zerodayinitiative.com/advisories/ZDI-23-1765/
https://www.zerodayinitiative.com/advisories/ZDI-23-1766/

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

Identifikátor

Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj prehliadač Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v komponente V8, 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

12.12.2023

CVE

CVE-2023-6702, CVE-2023-6703, CVE-2023-6704, CVE-2023-6705, CVE-2023-6706, CVE-2023-6707

Zasiahnuté systémy

Chrome pre Mac a Linux vo verzii staršej ako 120.0.6099.109
Chrome pre Windows vo verzii staršej ako 120.0.6099.109/110

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/2023/12/stable-channel-update-for-desktop_12.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/274807

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

Identifikátor

Palo Alto Networks PAN-OS - bezpečnostná zraniteľnosť

Popis

Spoločnosť Palo Alto Networks vydala bezpečnostné aktualizácie na produkt PAN-OS, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.12.2023

CVE

CVE-2023-6790

Zasiahnuté systémy

PAN-OS 11.0 vo verziách starších 11.0.1
PAN-OS 10.2 vo verziách starších 10.2.4
PAN-OS 10.1 vo verziách starších 10.1.9
PAN-OS 10.0 vo verziách starších 10.0.12
PAN-OS 9.1 vo verziách starších 9.1.16
PAN-OS 9.0 vo verziách starších 9.0.17
PAN-OS 8.1 vo verziách starších 8.1.25

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://security.paloaltonetworks.com/CVE-2023-6790

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

Identifikátor

pfSense - tri bezpečnostné zraniteľnosti

Popis

Vývojári open source firewallu pfSense vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov 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

12.12.2023

CVE

CVE-2023-42325, CVE-2023-42326, CVE-2023-42327

Zasiahnuté systémy

pfSense CE vo verzii staršej ako 2.7.1
pfSense Plus vo verzii staršej ako 23.09

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://thehackernews.com/2023/12/new-security-vulnerabilities-uncovered.html
https://www.sonarsource.com/blog/pfsense-vulnerabilities-sonarcloud/

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

Identifikátor

HPE Cray Programming Environment Slurm - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostnú aktualizáciu na svoj produkt Cray Programming Environment Slurm, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom SQL injekcie vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Ostatné zraniteľnosti možno zneužiť na získanie neoprávneného prístupu k citlivým údajom alebo zneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.12.2023

CVE

CVE-2023-41914, CVE-2023-49933, CVE-2023-49934, CVE-2023-49935, CVE-2023-49936, CVE-2023-49937, CVE-2023-49938

Zasiahnuté systémy

HPE Cray Programming Environment Slurm vo verzii 22.10 až 23.05 (vrátane)

Následky

Vykonanie škodlivého kódu a 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 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://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbcr04583en_us

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

Identifikátor

Apache Dubbo - bezpečnostná zraniteľnosť

Popis

Vývojári frameworku Apache Dubbo 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

15.12.2023

CVE

CVE-2023-46279

Zasiahnuté systémy

Apache Dubbo vo verzii staršej ako 3.2.10

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://lists.apache.org/thread/zw53nxrkrfswmk9n3sfwxmcj7x030nmo
https://dubbo.apache.org/en/download/
https://exchange.xforce.ibmcloud.com/vulnerabilities/275111

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

Identifikátor

Dell PowerProtect DD - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Dell vydala bezpečnostné aktualizácie na svoj produkt PowerProtect DD, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.12.2023

CVE

CVE-2023-44277, CVE-2023-44278, CVE-2023-44279, CVE-2023-44284, CVE-2023-44285, CVE-2023-44286, CVE-2023-48667, CVE-2023-48668

Zasiahnuté systémy

Dell PowerProtect DD vo verzii staršej ako 7.13.0.10, LTS 7.7.5.25, LTS 7.10.1.15 a 6.2.1.110

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 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.dell.com/support/kbdoc/en-us/000220264/dsa-2023-412-dell-technologies-powerprotect-security-update-for-multiple-security-vulnerabilities
https://exchange.xforce.ibmcloud.com/vulnerabilities/275098

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

Identifikátor

X.Org X server - dve bezpečnostné zraniteľnosti

Popis

Vývojári projektu X.Org X server vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zneužitia out-of-bounds zápisu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.12.2023

CVE

CVE-2023-6377, CVE-2023-6478

Zasiahnuté systémy

X.Org X server vo verzii staršej ako 21.1.10
Xwayland vo verzii staršej ako 23.2.3

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

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/q4/270
https://exchange.xforce.ibmcloud.com/vulnerabilities/274864
https://exchange.xforce.ibmcloud.com/vulnerabilities/274857

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

Identifikátor

Fortinet produkty - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Fortinet vydala bezpečnostné aktualizácie na produkty FortiOS, FortiPAM a FortiProxy, ktoré opravujú tri bezpečnostné zraniteľnosti.
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

12.12.2023

CVE

CVE-2023-36639, CVE-2023-41678, CVE-2023-47536

Zasiahnuté systémy

FortiOS 6.0 vo všetkých verziách
FortiOS 6.2 vo verzii staršej ako 6.2.16
FortiOS 6.4 vo všetkých verziách
FortiOS 7.0 vo všetkých verziách
FortiOS 7.2 vo verzii staršej ako 7.2.5
FortiOS 7.4 vo verzii staršej ako 7.4.1
FortiPAM 1.0 vo všetkých verziách
FortiPAM 1.1 vo verzii staršej ako 1.1.2
FortiProxy 2.0 vo verzii staršej ako 2.0.13
FortiProxy 7.0 vo verzii staršej ako 7.0.11
FortiProxy 7.2 vo verzii staršej ako 7.2.5

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.fortiguard.com/psirt/FG-IR-23-196
https://www.fortiguard.com/psirt/FG-IR-23-432
https://www.fortiguard.com/psirt/FG-IR-23-138

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

Identifikátor

Parallels Desktop - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Parallels International vydala bezpečnostnú aktualizáciu na svoj produkt Parallels Desktop, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, 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

19.10.2023

CVE

CVE-2023-50226, CVE-2023-50227, CVE-2023-50228

Zasiahnuté systémy

Parallels Desktop vo verzii staršej ako 19.1.0 (54729)

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://kb.parallels.com/en/125013#section1
https://www.zerodayinitiative.com/advisories/ZDI-23-1804/
https://www.zerodayinitiative.com/advisories/ZDI-23-1805/
https://www.zerodayinitiative.com/advisories/ZDI-23-1803/

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

Identifikátor

FXC AE1021PE a AE1021 - bezpečnostná zraniteľnosť

Popis

Spoločnosť FXC vydala bezpečnostnú aktualizáciu na svoje produkty AE1021PE a AE1021, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje autentifikovanému útočníkovi s právomocami používateľa, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.12.2023

CVE

CVE-2023-49897

Zasiahnuté systémy

AE1021PE a AE1021 vo verzii staršej ako 2.0.10

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/273276

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

Identifikátor

Check Point Harmony Endpoint/ZoneAlarm Extreme Security - bezpečnostná zraniteľnosť

Popis

Spoločnosť Check Point vydala bezpečnostnú aktualizáciu na svoje produkty Harmony Endpoint a ZoneAlarm Extreme Security, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.11.2023

CVE

CVE-2023-28134

Zasiahnuté systémy

Enterprise Endpoint Security vo verziách starších ako E87.10 Windows Clients

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://support.checkpoint.com/results/sk/sk181597
https://www.zerodayinitiative.com/advisories/ZDI-23-1764/

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

Identifikátor

Adobe produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje portfólio produktov, 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

12.12.2023

CVE

CVE-2023-44362, CVE-2023-47061, CVE-2023-47062, CVE-2023-47078, CVE-2023-47079, CVE-2023-47080, CVE-2023-47081, CVE-2023-48440, CVE-2023-48441, CVE-2023-48442, CVE-2023-48443, CVE-2023-48444, CVE-2023-48445, CVE-2023-48446, CVE-2023-48447, CVE-2023-48448, CVE-2023-48449, CVE-2023-48450, CVE-2023-48451, CVE-2023-48452, CVE-2023-48453, CVE-2023-48454, CVE-2023-48455, CVE-2023-48456, CVE-2023-48457, CVE-2023-48458, CVE-2023-48459, CVE-2023-48460, CVE-2023-48461, CVE-2023-48462, CVE-2023-48463, CVE-2023-48464, CVE-2023-48465, CVE-2023-48466, CVE-2023-48467, CVE-2023-48468, CVE-2023-48469, CVE-2023-4847, CVE-2023-48470, CVE-2023-48471, CVE-2023-48472, CVE-2023-48473, CVE-2023-48474, CVE-2023-48475, CVE-2023-48476, CVE-2023-48477, CVE-2023-48478, CVE-2023-48479, CVE-2023-48480, CVE-2023-48481, CVE-2023-48482, CVE-2023-48483, CVE-2023-48484, CVE-2023-48485, CVE-2023-48486, CVE-2023-48487, CVE-2023-48488, CVE-2023-48489, CVE-2023-48490, CVE-2023-48491, CVE-2023-48492, CVE-2023-48493, CVE-2023-48494, CVE-2023-48495, CVE-2023-48496, CVE-2023-48497, CVE-2023-48498, CVE-2023-48499, CVE-2023-48500, CVE-2023-48501, CVE-2023-48502, CVE-2023-48503, CVE-2023-48504, CVE-2023-48505, CVE-2023-48506, CVE-2023-48507, CVE-2023-48508, CVE-2023-48509, CVE-2023-48510, CVE-2023-48511, CVE-2023-48512, CVE-2023-48513, CVE-2023-48514, CVE-2023-48515, CVE-2023-48516, CVE-2023-48517, CVE-2023-48518, CVE-2023-48519, CVE-2023-48520, CVE-2023-48521, CVE-2023-48522, CVE-2023-48523, CVE-2023-48524, CVE-2023-48525, CVE-2023-48526, CVE-2023-48527, CVE-2023-48528, CVE-2023-48529, CVE-2023-48530, CVE-2023-48531, CVE-2023-48532, CVE-2023-48533, CVE-2023-48534, CVE-2023-48535, CVE-2023-48536, CVE-2023-48537, CVE-2023-48538, CVE-2023-48539, CVE-2023-48540, CVE-2023-48541, CVE-2023-48542, CVE-2023-48543, CVE-2023-48544, CVE-2023-48545, CVE-2023-48546, CVE-2023-48547, CVE-2023-48548, CVE-2023-48549, CVE-2023-48550, CVE-2023-48551, CVE-2023-48552, CVE-2023-48553, CVE-2023-48554, CVE-2023-48555, CVE-2023-48556, CVE-2023-48557, CVE-2023-48558, CVE-2023-48559, CVE-2023-48560, CVE-2023-48561, CVE-2023-48562, CVE-2023-48563, CVE-2023-48564, CVE-2023-48565, CVE-2023-48566, CVE-2023-48567, CVE-2023-48568, CVE-2023-48569, CVE-2023-48570, CVE-2023-48571, CVE-2023-48572, CVE-2023-48573, CVE-2023-48574, CVE-2023-48575, CVE-2023-48576, CVE-2023-48577, CVE-2023-48578, CVE-2023-48579, CVE-2023-48580, CVE-2023-48581, CVE-2023-48582, CVE-2023-48583, CVE-2023-48584, CVE-2023-48585, CVE-2023-48586, CVE-2023-48587, CVE-2023-48588, CVE-2023-48589, CVE-2023-48590, CVE-2023-48591, CVE-2023-48592, CVE-2023-48593, CVE-2023-48594, CVE-2023-48595, CVE-2023-48596, CVE-2023-48597, CVE-2023-48598, CVE-2023-48599, CVE-2023-48600, CVE-2023-48601, CVE-2023-48602, CVE-2023-48603, CVE-2023-48604, CVE-2023-48605, CVE-2023-48606, CVE-2023-48607, CVE-2023-48608, CVE-2023-48609, CVE-2023-48610, CVE-2023-48611, CVE-2023-48612, CVE-2023-48613, CVE-2023-48614, CVE-2023-48615, CVE-2023-48616, CVE-2023-48617, CVE-2023-48618, CVE-2023-48619, CVE-2023-48620, CVE-2023-48621, CVE-2023-48622, CVE-2023-48623, CVE-2023-48624, CVE-2023-48625, CVE-2023-48626, CVE-2023-48627, CVE-2023-48628, CVE-2023-48629, CVE-2023-48630, CVE-2023-48632, CVE-2023-48633, CVE-2023-48634, CVE-2023-48635, CVE-2023-48636, CVE-2023-48637, CVE-2023-48638, CVE-2023-48639

Zasiahnuté systémy

Adobe Substance 3D Designer vo verzii staršej ako 13.1.0
Adobe After Effects vo verzii staršej ako 23.6.2
Adobe After Effects vo verzii staršej ako 24.1
Adobe Substance 3D Sampler vo verzii staršej ako 4.2.2
Adobe Substance 3D Stager vo verzii staršej ako 2.1.3
Adobe Experience Manager (AEM) vo verzii staršej ako 6.5.19.0
Adobe Dimension vo verzii staršej ako 3.4.11
Adobe InDesign vo verzii staršej ako ID19.1
Adobe InDesign vo verzii staršej ako ID18.5.1
Illustrator 2023 vo verzii staršej ako 27.9.1
Illustrator 2024 vo verzii staršej ako 28.1
Adobe Prelude vo verzii staršej ako 22.6.1

Následky
Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému Neoprávnený prístup k citlivým údajom

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://helpx.adobe.com/security/products/substance3d_designer/apsb23-76.html https://helpx.adobe.com/security/products/after_effects/apsb23-75.html https://helpx.adobe.com/security/products/substance3d-sampler/apsb23-74.html https://helpx.adobe.com/security/products/substance3d_stager/apsb23-73.html https://helpx.adobe.com/security/products/experience-manager/apsb23-72.html https://helpx.adobe.com/security/products/dimension/apsb23-71.html https://helpx.adobe.com/security/products/indesign/apsb23-70.html https://helpx.adobe.com/security/products/prelude/apsb23-67.html https://github.com/advisories/GHSA-c494-g465-3396

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

Identifikátor

Intel Driver & Support Assistant - zero day bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zero day zraniteľnosti produktu Intel Driver & Support Assistant.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom symbolického odkazu eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.12.2023

CVE

CVE-2023-50197

Zasiahnuté systémy

Intel Driver & Support Assistant vo verzii staršej ako 23.4.39 (vrátane)

Následky

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

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://www.zerodayinitiative.com/advisories/ZDI-23-1773/

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

Identifikátor

Cambium ePMP 5GHz Force 300-25 - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Cambium ePMP 5GHz Force 300-25.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov 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

14.12.2023

CVE

CVE-2023-6691

Zasiahnuté systémy

ePMP Force 300-25 vo verzii staršej ako 4.7.0.1 (vrátane)

Následky

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

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://www.cisa.gov/news-events/ics-advisories/icsa-23-348-01

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

Identifikátor

Ivanti Avalanche - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Ivanti vydala bezpečnostnú aktualizáciu na svoj produkt Avalanche, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.12.2023

CVE

CVE-2022-43554, CVE-2022-43555, CVE-2023-32567, CVE-2023-41725, CVE-2023-41726

Zasiahnuté systémy

Ivanti Avalanche vo verzii staršej ako v6.4.1.236

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 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://download.wavelink.com/Files/avalanche_v6.4.1.236_release_notes.txt
https://www.zerodayinitiative.com/advisories/ZDI-23-1799/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Progress Software WhatsUp Gold - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Progress Software vydala bezpečnostnú aktualizáciu na svoj nástroj na monitorovanie siete WhatsUp Gold, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom injekcie škodlivého skriptu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.12.2023

CVE

CVE-2023-6364, CVE-2023-6365, CVE-2023-6366, CVE-2023-6367, CVE-2023-6368, CVE-2023-6595

Zasiahnuté systémy

WhatsUp Gold vo verzii staršej ako 2023.1

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://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-December-2023
https://exchange.xforce.ibmcloud.com/vulnerabilities/275260

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

Identifikátor

Bosch produkty - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Bosch vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú tri bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produktoch, ktoré využívajú BT software ako server alebo klient, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Zraniteľnosti v IP kamerách produktovej rady CPP13 a CPP14 by vzdialený autentifikovaný útočník s právomocami administrátora mohol zneužiť na vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.12.2023

CVE

CVE-2023-32230, CVE-2023-35867, CVE-2023-39509

Zasiahnuté systémy
CPP13 vo verzii firmvéru staršej ako 8.90.0037 CPP14 vo verzii firmvéru staršej ako 9.00.0210 BIS Video Engine bez aplikovanej záplaty BIS 5.0.1 mandatory common files 1 for Patch Release for CVE-2023-35867 BIS Video Engine bez aplikovanej záplaty BIS 5.0.1 mandatory common files 2 for Patch Release for CVE-2023-35867 BIS Video Engine bez aplikovanej záplaty BIS 5.0.1 files for language xx for Patch Release for CVE-2023-35867 BVMS Viewer bez aplikovanej záplaty BVMS111165_VWR_Patch_FW90improve_434923,428521.zip BVMS Viewer bez aplikovanej záplaty BVMS Viewer 12.0.1 BVMS bez aplikovanej záplaty BVMS111165_Patch_FW90improve_434923,428521.zip BVMS bez aplikovanej záplaty BVMS 12.0.1 Configuration Manager vo verzii staršej ako 7.70.0090 DIVAR IP all-in-one 7000 R3 bez aplikovanej záplaty BVMS_11.1.1_Updates_SystemManager_package_1.2.zip DIVAR IP all-in-one 7000 R3 bez aplikovanej záplaty BVMS 12.0.1 DIVAR IP 7000 R2 bez aplikovanej záplaty BVMS - BVMS111165_Patch_FW90improve_434923,428521.zip DIVAR IP 7000 R2 bez aplikovanej záplaty BVMS 12.0.1 DIVAR IP all-in-one 5000 bez aplikovanej záplaty BVMS_11.1.1_Updates_SystemManager_package_1.2.zip DIVAR IP all-in-one 5000 bez aplikovanej záplaty BVMS 12.0.1 DIVAR IP all-in-one 7000 bez aplikovanej záplaty BVMS_11.1.1_Updates_SystemManager_package_1.2.zip DIVAR IP all-in-one 7000 bez aplikovanej záplaty BVMS 12.0.1 DIVAR IP all-in-one 4000 bez aplikovanej záplaty BVMS_11.1.1_Updates_SystemManager_package_1.2.zip DIVAR IP all-in-one 4000 bez aplikovanej záplaty BVMS 12.0.1 DIVAR IP all-in-one 6000 bez aplikovanej záplaty BVMS_11.1.1_Updates_SystemManager_package_1.2.zip DIVAR IP all-in-one 6000 bez aplikovanej záplaty BVMS 12.0.1 Intelligent Insights vo verzii staršej ako 1.0.3.22 Monitorwall - záplata je v príprave ONVIF Camera Event Driver Tool vo verzii staršej ako 2.1.1.4 Project Assistant vo verzii staršej ako 2.4.0.36 Video Security Client vo verzii staršej ako 3.4.0.42 Video Streaming Gateway (VSG) vo verzii staršej ako 8.1.4.1 Video Streaming Gateway (VSG) vo verzii staršej ako 9.1.0.12 Video Recording Manager (VRM) vo verzii staršej ako 04.04.0027 Video Recording Manager (VRM) vo verzii staršej ako 04.20.0016 VJD-7513 vo verzii staršej ako 10.40.0061 VJD-7523 vo verzii staršej ako 10.40.0061

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

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://psirt.bosch.com/security-advisories/bosch-sa-092656-bt.html
https://psirt.bosch.com/security-advisories/bosch-sa-638184-bt.html

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

Identifikátor

Johnson Controls Kantech Gen1 ioSmart - bezpečnostná zraniteľnosť

Popis

Spoločnosť Johnson Controls vydala bezpečnostnú aktualizáciu na svoj produkt Kantech Gen1 ioSmart, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi s fyzickým prístupom k zariadeniu prístup ku komunikačnej pamäti čítačky a získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

14.12.2023

CVE

CVE-2023-0248

Zasiahnuté systémy

Kantech Gen1 ioSmart card reader vo verzii firmvéru staršej ako 1.7.2

Následky

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-23-348-02

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

Identifikátor

Zoom produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Zoom vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

12.12.2023

CVE

CVE-2023-43583, CVE-2023-43585, CVE-2023-43586, CVE-2023-49646

Zasiahnuté systémy

Zoom Desktop Client pre Windows vo verzii staršej ako 5.16.5
Zoom VDI Client vo verzii staršej ako 5.16.0 (vynímajúc 5.14.14 a 5.15.12)
Zoom Video SDK pre Windows vo verzii staršej ako 5.16.5
Zoom Meeting SDK pre Windows vo verzii staršej ako 5.16.5
Zoom Mobile App pre Android vo verzii staršej ako 5.16.0
Zoom Mobile App pre iOS vo verzii staršej ako 5.16.0
Zoom Video SDK pre Android vo verzii staršej ako 5.16.0
Zoom Video SDK pre iOS vo verzii staršej ako 5.16.0
Zoom Meeting SDK pre Android vo verzii staršej ako 5.16.0
Zoom Meeting SDK pre iOS vo verzii staršej ako 5.16.0
Zoom Mobile App pre iOS vo verzii staršej ako 5.16.5
Zoom Video SDK pre iOS vo verzii staršej ako 5.16.5
Zoom Meeting SDK pre iOS vo verzii staršej ako 5.16.5
Zoom Desktop Client pre macOS vo verzii staršej ako 5.16.5
Zoom Mobile App pre Android vo verzii staršej ako 5.16.5
Zoom Desktop Client pre Linux vo verzii staršej ako 5.16.5
Zoom VDI Client vo verzii staršej ako 5.16.5 (vynímajúc 5.14.14 a 5.15.12)
Zoom SDKs vo verzii staršej ako 5.16.5

Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
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.zoom.com/en/trust/security-bulletin/ZSB-23062/ https://www.zoom.com/en/trust/security-bulletin/ZSB-23058/ https://www.zoom.com/en/trust/security-bulletin/ZSB-23059/ https://www.zoom.com/en/trust/security-bulletin/ZSB-23056/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.0
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

PaperCut MF a NG - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť ITS vydala bezpečnostnú aktualizáciu na svoj produkt PaperCut, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorených súborov eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Pre zneužitie zraniteľnosti musí byť spustená funkcia Print Archiving bez nainštalovaného GhostTrap.

Dátum prvého zverejnenia varovania

15.12.2023

CVE

CVE-2023-39471, CVE-2023-6006

Zasiahnuté systémy

PaperCut NG/MF Application Server pre Windows vo verzii staršej ako 23.0.1

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 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.papercut.com/kb/Main/security-bulletin-november-2023/
https://www.zerodayinitiative.com/advisories/ZDI-23-1798/

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-1447

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

Identifikátor

OpenAI ChatGPT - zero day bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu ChatGPT.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne upravených príkazov získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

13.12.2023

CVE

-

Zasiahnuté systémy

GPT vo verzii staršej ako 4 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Vzhľadom na absenciu aktualizácií mitigujúcich danú zraniteľnosť, bezpečnostní výskumníci odporúčajú dočasne obmedziť interakciu s predmetnou aplikáciou.
Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-23-1772/