BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 01. 2024 - 16. 01. 2024

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Zoom Desktop Client for Windows - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	Tenda AX1803 - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Paessler PRTG Network Monitor - bezpečnostná zraniteľnosť	Vysoká	**8.8**
04.	Popup Builder WP plugin - bezpečnostná zraniteľnosť	Vysoká	**8.8**
05.	Apple Magic Keyboard - bezpečnostná zraniteľnosť	Vysoká	**8.4**
06.	FortiOS a FortiProxy - bezpečnostná zraniteľnosť	Vysoká	**8.3**
07.	BCC Termostaty - bezpečnostná zraniteľnosť	Vysoká	**8.3**
08.	Kyocera Device Manager - bezpečnostná zraniteľnosť	Vysoká	**8.1**
09.	Intel produkty - viacero bezpečnostných zraniteľností	Vysoká	**7.9**
10.	Panasonic Control FPWIN Pro7 - dve bezpečnostné zraniteľnosti	Vysoká	**7.8**
11.	Linux kernel - tri bezpečnostné zraniteľnosti	Vysoká	**7.8**
12.	Horner Automation Cscape - bezpečnostná zraniteľnosť	Vysoká	**7.8**
13.	Schneider Electric Easergy Studio - bezpečnostná zraniteľnosť	Vysoká	**7.8**
14.	Adobe Substance 3D Stager - viacero bezpečnostných zraniteľností	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-1484

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

Identifikátor

Zoom Desktop Client for Windows - bezpečnostná zraniteľnosť

Popis

Spoločnosť Zoom Video Communications vydala bezpečnostné aktualizácie na svoje portfólio produktov, 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 získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

09.01.2024

CVE

CVE-2023-49647

Zasiahnuté systémy

Zoom Desktop Client pre Windows vo verzii staršej ako 5.16.10
VDI Client pre Windows vo verzii staršej ako 5.16.10 (vynímajúc 5.14.14 a 5.15.12)
Zoom Video SDK pre Windows vo verzii staršej ako 5.16.10
Zoom Meeting SDK pre Windows vo verzii staršej ako 5.16.10

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://www.zoom.com/en/trust/security-bulletin/ZSB-24001/

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

Identifikátor

Tenda AX1803 - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach routra Tenda AX1803.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje útočníkovi nachádzajúcemu sa 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

10.01.2024

CVE

CVE-2023-51952, CVE-2023-51953, CVE-2023-51954, CVE-2023-51955, CVE-2023-51956, CVE-2023-51957, CVE-2023-51958, CVE-2023-51959, CVE-2023-51960, CVE-2023-51961, CVE-2023-51962, CVE-2023-51963, CVE-2023-51964, CVE-2023-51965, CVE-2023-51966, CVE-2023-51967, CVE-2023-51968, CVE-2023-51969, CVE-2023-51970, CVE-2023-51971, CVE-2023-51972

Zasiahnuté systémy

Tenda AX1803 vo verzii firmvéru staršej ako 1.0.0.1 (vrátane)

Následky

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

Odporúčania

Vzhľadom na to, že produkt už nie je udržiavaný, odporúčame prejsť na iný produkt s platnou podporou.
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://grove-laser-8ad.notion.site/Tenda-AX1803-Buffer-Overflow-in-formSetIptv-d758f5dba8f646afaf5cddc6f8d3ec70
https://exchange.xforce.ibmcloud.com/vulnerabilities/279092
https://exchange.xforce.ibmcloud.com/vulnerabilities/279101
https://exchange.xforce.ibmcloud.com/vulnerabilities/279102
https://exchange.xforce.ibmcloud.com/vulnerabilities/279103
https://exchange.xforce.ibmcloud.com/vulnerabilities/279104
https://exchange.xforce.ibmcloud.com/vulnerabilities/279109
https://exchange.xforce.ibmcloud.com/vulnerabilities/279116
https://exchange.xforce.ibmcloud.com/vulnerabilities/279119
https://exchange.xforce.ibmcloud.com/vulnerabilities/279122
https://exchange.xforce.ibmcloud.com/vulnerabilities/279123
https://exchange.xforce.ibmcloud.com/vulnerabilities/279134
https://exchange.xforce.ibmcloud.com/vulnerabilities/279135
https://exchange.xforce.ibmcloud.com/vulnerabilities/279136

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

Identifikátor

Paessler PRTG Network Monitor - bezpečnostná zraniteľnosť

Popis

Spoločnosť Paessler vydala bezpečnostnú aktualizáciu na svoj produkt PRTG Network Monitor, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom XSS (Cross-Site Scripting) útoku získať neoprávnený prístup do systému. Zneužitie zrantieľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

15.01.2024

CVE

CVE-2023-51630

Zasiahnuté systémy

PRTG Network Monitor vo verzii staršej ako 24.1.90.1306

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://www.paessler.com/prtg/history/stable
https://www.zerodayinitiative.com/advisories/ZDI-24-073/

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

Identifikátor

Popup Builder WP plugin - bezpečnostná zraniteľnosť

Popis

Vývojári WordPress pluginu Popup Builder vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom XSS (Cross-Site Scripting) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.12.2023

CVE

CVE-2023-6000

Zasiahnuté systémy

Popup Builder plugin vo verzii staršej ako 4.2.3

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://wpscan.com/blog/stored-xss-fixed-in-popup-builder-4-2-3/
https://thehackernews.com/2024/01/balada-injector-infects-over-7100.html
https://blog.sucuri.net/2024/01/thousands-of-sites-with-popup-builder-compromised-by-balada-injector.html

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

Identifikátor

Apple Magic Keyboard - bezpečnostná zraniteľnosť

Popis

Spoločnosť Apple vydala bezpečnostnú aktualizáciu na svoj produkt Magic Keyboard, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkov s fyzickým prístupom k zraniteľnému zariadeniu získať neoprávnený prístup k citlivým údajom (Bluetooth pairing key) a tie následne zneužiť na monitorovanie Bluetooth komunikácie.

Dátum prvého zverejnenia varovania

11.01.2024

CVE

CVE-2024-0230

Zasiahnuté systémy

Apple Magic Keyboard vo verzii staršej ako 2.0.6

Následky

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://support.apple.com/en-us/HT214050

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

Identifikátor

FortiOS a FortiProxy - bezpečnostná zraniteľnosť

Popis

Spoločnosť Fortinet vydala bezpečnostné aktualizácie na svoje produkty FortiOS a FortiProxy, ktoré opravujú bezpečnostnú zraniteľnosť.
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 vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

09.01.2024

CVE

CVE-2023-44250

Zasiahnuté systémy

FortiOS 7.4 vo verzii staršej ako 7.4.2
FortiOS 7.2 vo verzii staršej ako 7.2.6
FortiProxy 7.4 vo verzii staršej ako 7.4.2

Následky

Eskalácia privilégií
Vykonanie škodlivého kódu s následkom úplného narušenia 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.fortiguard.com/psirt/FG-IR-23-315

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

Identifikátor

BCC Termostaty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Bosch vydala bezpečnostnú aktualizáciu na svoje portfólio termostatov BCC, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente voľný prístup do systému prostredníctvom otvoreného portu 8899, a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

09.01.2024

CVE

CVE-2023-49722

Zasiahnuté systémy

Termostaty Bosch rady BCC vo verzii staršej ako v4.13.33

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://psirt.bosch.com/security-advisories/bosch-sa-473852.html

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

Identifikátor

Kyocera Device Manager - bezpečnostná zraniteľnosť

Popis

Spoločnosť Kyocera vydala bezpečnostnú aktualizáciu na svoj produkt Device Manager, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

22.12.2023

CVE

CVE-2023-50916

Zasiahnuté systémy

Kyocera Device Manager vo verzii staršej ako 3.1.1213.0

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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.kyoceradocumentsolutions.us/en/about-us/pr-and-award-certifications/press/kyocera-device-manager-cve-2023-50196-vulnerability-solution-update.html
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/cve-2023-50916-authentication-coercion-vulnerability-in-kyocera-device-manager/
https://www.csoonline.com/article/1288855/enterprises-with-kyocera-printers-open-to-path-traversal-attacks.html
https://thehackernews.com/2024/01/alert-new-vulnerabilities-discovered-in.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.9
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Intel produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Intel vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v NUC Software, spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa vykonať neoprávnené zmeny v systéme a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

09.01.2024

CVE

CVE-2023-28722, CVE-2023-28738, CVE-2023-28743, CVE-2023-29244, CVE-2023-29495, CVE-2023-32272, CVE-2023-32544, CVE-2023-38541, CVE-2023-38587, CVE-2023-42429, CVE-2023-42766

Zasiahnuté systémy

Intel® NUC
Intel® NUC Software
Intel® NUC BIOS Firmware

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v časti ZDROJE.

Následky

Esklácia privilégií
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Bezpečnostná záplata je obsiahnutá v aktualizácii UEFI BIOS, preto používateľom odporúčame nainštalovať aktualizácie systému UEFI BIOS z webových stránok výrobcu pre ich konkrétne elektronické zariadenie. V prípade, že prevádzkujete fyzické servery s operačným systémom Linux, uistite sa, že máte nainštalovaný balík intel-microcode. Na BSD systémoch môžete použiť balík cpupdate.

Zdroje

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00964.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html

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

Identifikátor

Panasonic Control FPWIN Pro7 - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Panasonic vydala bezpečnostnú aktualizáciu na svoj produkt Control FPWIN Pro7, ktorá opravuje dve bezpečnostné zraniteľnosti.
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

09.01.2024

CVE

CVE-2023-6314, CVE-2023-6315

Zasiahnuté systémy

Panasonic Control FPWIN Pro7 vo verzii staršej ako 7.7.1.0

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www3.panasonic.biz/ac/ae/dl/software/index.jsp?series_cd=3359
http://jvn.jp/en/vu/JVNVU92102247/index.html

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

Identifikátor

Linux kernel - tri bezpečnostné zraniteľnosti

Popis

Vývojári jadra operačného systému Linux vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej 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

09.01.2024

CVE

CVE-2023-6546, CVE-2024-0562, CVE-2024-0565

Zasiahnuté systémy

Linux kernel vo verzii master commitu staršej ako 6.7-rc6

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://github.com/torvalds/linux/commit/3c4f8333b582487a2d1e02171f1465531cde53e3
https://exchange.xforce.ibmcloud.com/vulnerabilities/275779
https://exchange.xforce.ibmcloud.com/vulnerabilities/279419
https://exchange.xforce.ibmcloud.com/vulnerabilities/279430

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

Identifikátor

Horner Automation Cscape - bezpečnostná zraniteľnosť

Popis

Spoločnosť Horner Automation vydala bezpečnostnú aktualizáciu na svoj produkt Cscape, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených CSP súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.01.2024

CVE

CVE-2023-7206

Zasiahnuté systémy

Horner Automation Cscape vo verzii staršej ako v9.90 SP11

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-24-011-04

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

Identifikátor

Schneider Electric Easergy Studio - bezpečnostná zraniteľnosť

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoj produkt Easergy Studio, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepristupnenie služby.

Dátum prvého zverejnenia varovania

11.01.2024

CVE

CVE-2023-7032

Zasiahnuté systémy

Easergy Studio vo verzii staršej ako 9.3.6

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-24-011-05

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

Identifikátor

Adobe Substance 3D Stager - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Adobe vydala bezpečnostnú aktualizáciu na svoj produkt Substance 3D Stager, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

09.01.2024

CVE

CVE-2024-20710, CVE-2024-20711, CVE-2024-20712, CVE-2024-20713, CVE-2024-20714, CVE-2024-20715

Zasiahnuté systémy

Adobe Substance 3D Stager vo verzii staršej ako 2.1.4

Následky

Neoprávnený prístup k citlivým údajom
Vykonanie škodlivého kódu

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://helpx.adobe.com/security/products/substance3d_stager/apsb24-06.html