BEZPEČNOSTNÝ BULLETIN

Týždeň 12. 07. 2023 - 18. 07. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01794/2022/SK-CERT-1234

BEZPEČNOSTNÝ BULLETIN

Týždeň 12. 07. 2023 - 18. 07. 2023

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

Identifikátor

Zimbra - zero-day bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Zimbra.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených XML súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

13.07.2023

CVE

-

Zasiahnuté systémy

Zimbra Collaboration Suite vo verzii 8.8.15

Následky

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

Odporúčania

Na uvedenú zraniteľnosť nie sú v súčasnosti dostupné aktualizácie. Výrobca odporúča do vydania záplat zraniteľnosť mitigovať podľa postupu, ktorý môžete nájsť na webovej adrese produktu ZIMBRA uvedenej v časti ZDROJE.

Zdroje

https://blog.zimbra.com/2023/07/security-update-for-zimbra-collaboration-suite-version-8-8-15/
https://www.malwarebytes.com/blog/news/2023/07/act-now-unpatched-zimbra-vulnerability-is-actively-exploited

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

Identifikátor

Firefox, Firefox ESR - bezpečnostná zraniteľnosť

Popis

Spoločnosť Mozilla Foundation vydala bezpečnostné aktualizácie na produkty Mozilla Firefox a Firefox ESR, 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

11.07.2023

CVE

CVE-2023-3600

Zasiahnuté systémy

Firefox vo verzii staršej ako 115.0.2
Firefox ESR vo verzii staršej ako 115.0.2

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://www.mozilla.org/en-US/security/advisories/mfsa2023-26/
https://www.cybersecurity-help.cz/vdb/SB2023071154

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

Identifikátor

HPE ArubaOS a SD-WAN - viacero bezpečnostných zraniteľností

Popis

Spoločnosť HPE vydala bezpečnostnú aktualizáciu na svoje produkt ArubaOS a SD-WAN, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.07.2023

CVE

CVE-2023-35971, CVE-2023-35972, CVE-2023-35973, CVE-2023-35974, CVE-2023-35975, CVE-2023-35976, CVE-2023-35977, CVE-2023-35978, CVE-2023-35979

Zasiahnuté systémy

ArubaOS 10.4.x.x: vo verzii staršej ako 10.4.0.2
ArubaOS 8.11.x.x: vo verzii staršej ako 8.11.1.1
ArubaOS 8.10.x.x: vo verzii staršej ako 8.10.0.7
ArubaOS 8.6.x.x: vo verzii staršej ako 8.6.0.21
ArubaOS 8.9.x.x vo všetkých verziách
ArubaOS 8.8.x.x vo všetkých verziách
ArubaOS 8.7.x.x vo všetkých verziách
ArubaOS 6.5.4.x vo všetkých verziách
SD-WAN 8.7.0.0-2.3.0.x vo všetkých verziách
SD-WAN 8.6.0.4-2.2.x.x vo všetkých verziách

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.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04490en_us

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.4
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, ktoré opravujú 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 neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

11.07.2023

CVE

CVE-2023-34116, CVE-2023-34117, CVE-2023-34118, CVE-2023-34119, CVE-2023-36536, CVE-2023-36537, CVE-2023-36538

Zasiahnuté systémy

Zoom Desktop Client for Windows vo verzii staršej ako 5.15.0.
Zoom Client SDK vo verzii staršej ako 5.15.0
Zoom Rooms for Windows vo verzii staršej ako 5.15.0

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby
Eskalácia privilégií

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://explore.zoom.us/en/trust/security/security-bulletin/

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

Identifikátor

IBM Facsimile Support for i - bezpečnostná zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Facsimile Support for i, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi 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

17.07.2023

CVE

CVE-2023-30988

Zasiahnuté systémy

IBM i vo verzii staršej ako 7.5 s nainštalovaným 5798-FAX vo verzii V5R8M0
IBM i vo verzii staršej ako 7.4 s nainštalovaným 5798-FAX vo verzii V5R8M0
IBM i vo verzii staršej ako 7.3 s nainštalovaným 5798-FAX vo verzii V5R8M0
IBM i vo verzii staršej ako 7.2 s nainštalovaným 5798-FAX vo verzii V5R8M0

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.ibm.com/support/pages/node/7012355
https://exchange.xforce.ibmcloud.com/vulnerabilities/254016

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

Identifikátor

ROZCOM - dve bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach intercomov ROZCOM.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvolenými prihlasovacími údajmi a umožňuje lokálnemu, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

05.04.2023

CVE

CVE-2023-31184, CVE-2023-31185

Zasiahnuté systémy

Intercomy ROZCOM vo všetkých verziách

Následky

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. V prípade, že výmena systému nie je možná, odporúčame postupovať podľa pokynov bezpečnostných výskumníkov uvedených na odkazoch v sekcii ZDROJE.

Zdroje

https://claroty.com/team82/disclosure-dashboard/cve-2023-31184
https://research.checkpoint.com/2023/major-security-flaws-in-popular-quickblox-chat-and-video-framework-expose-sensitive-data-of-millions/

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

Identifikátor

Dassault Systemes Solidworks - viacero bezpečnostných zraniteľností

Popis

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

Dátum prvého zverejnenia varovania

12.07.2023

CVE

CVE-2023-2763

Zasiahnuté systémy

SOLIDWORKS vo verzii staršej ako 2023 (vrátane)

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-23-911/

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

Identifikátor

Kofax Power PDF - viacero bezpečnostných zraniteľností

Popis

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

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

Dátum prvého zverejnenia varovania

13.07.2023

CVE

CVE-2023-37330, CVE-2023-37331, CVE-2023-37332, CVE-2023-37333, CVE-2023-37334, CVE-2023-37335, CVE-2023-37336, CVE-2023-37337, CVE-2023-37338, CVE-2023-37339, CVE-2023-37340, CVE-2023-37341, CVE-2023-37342, CVE-2023-37343, CVE-2023-37344, CVE-2023-37345, CVE-2023-37346, CVE-2023-37347, CVE-2023-37348, CVE-2023-37349, CVE-2023-37350, CVE-2023-37351, CVE-2023-37352, CVE-2023-37353, CVE-2023-37354, CVE-2023-37355, CVE-2023-37356, CVE-2023-37357, CVE-2023-37358, CVE-2023-37359, CVE-2023-38077, CVE-2023-38078, CVE-2023-38079, CVE-2023-38080, CVE-2023-38081, CVE-2023-38082, CVE-2023-38083, CVE-2023-38084, CVE-2023-38085, CVE-2023-38086, CVE-2023-38087, CVE-2023-38088, CVE-2023-38089, CVE-2023-38090, CVE-2023-38092, CVE-2023-38093, CVE-2023-38094

Zasiahnuté systémy

Power PDF 5.0 Standard & Advanced vo verzii staršej ako v5.0.0.10.0.23307.

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-23-922/
https://www.zerodayinitiative.com/advisories/ZDI-23-923/
https://www.zerodayinitiative.com/advisories/ZDI-23-924/
https://www.zerodayinitiative.com/advisories/ZDI-23-925/
https://www.zerodayinitiative.com/advisories/ZDI-23-926/
https://www.zerodayinitiative.com/advisories/ZDI-23-927/
https://www.zerodayinitiative.com/advisories/ZDI-23-928/
https://www.zerodayinitiative.com/advisories/ZDI-23-929/
https://www.zerodayinitiative.com/advisories/ZDI-23-930/
https://www.zerodayinitiative.com/advisories/ZDI-23-931/
https://www.zerodayinitiative.com/advisories/ZDI-23-932/
https://www.zerodayinitiative.com/advisories/ZDI-23-933/
https://www.zerodayinitiative.com/advisories/ZDI-23-934/
https://www.zerodayinitiative.com/advisories/ZDI-23-935/
https://www.zerodayinitiative.com/advisories/ZDI-23-936/
https://www.zerodayinitiative.com/advisories/ZDI-23-937/
https://www.zerodayinitiative.com/advisories/ZDI-23-938/
https://www.zerodayinitiative.com/advisories/ZDI-23-939/
https://www.zerodayinitiative.com/advisories/ZDI-23-940/
https://www.zerodayinitiative.com/advisories/ZDI-23-941/
https://www.zerodayinitiative.com/advisories/ZDI-23-942/
https://www.zerodayinitiative.com/advisories/ZDI-23-943/
https://www.zerodayinitiative.com/advisories/ZDI-23-944/
https://www.zerodayinitiative.com/advisories/ZDI-23-945/
https://www.zerodayinitiative.com/advisories/ZDI-23-946/
https://www.zerodayinitiative.com/advisories/ZDI-23-947/
https://www.zerodayinitiative.com/advisories/ZDI-23-948/
https://www.zerodayinitiative.com/advisories/ZDI-23-949/
https://www.zerodayinitiative.com/advisories/ZDI-23-950/
https://www.zerodayinitiative.com/advisories/ZDI-23-951/
https://www.zerodayinitiative.com/advisories/ZDI-23-952/
https://www.zerodayinitiative.com/advisories/ZDI-23-953/
https://www.zerodayinitiative.com/advisories/ZDI-23-954/
https://www.zerodayinitiative.com/advisories/ZDI-23-955/
https://www.zerodayinitiative.com/advisories/ZDI-23-956/
https://www.zerodayinitiative.com/advisories/ZDI-23-957/
https://www.zerodayinitiative.com/advisories/ZDI-23-958/
https://www.zerodayinitiative.com/advisories/ZDI-23-959/
https://www.zerodayinitiative.com/advisories/ZDI-23-960/
https://www.zerodayinitiative.com/advisories/ZDI-23-961/
https://www.zerodayinitiative.com/advisories/ZDI-23-962/
https://www.zerodayinitiative.com/advisories/ZDI-23-963/
https://www.zerodayinitiative.com/advisories/ZDI-23-964/
https://www.zerodayinitiative.com/advisories/ZDI-23-965/
https://www.zerodayinitiative.com/advisories/ZDI-23-966/
https://www.zerodayinitiative.com/advisories/ZDI-23-967/
https://www.zerodayinitiative.com/advisories/ZDI-23-968/
https://www.zerodayinitiative.com/advisories/ZDI-23-969/

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

Identifikátor

Panasonic Control FPWIN Pro7 - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Panasonic vydala bezpečnostnú aktualizáciu na svoj programovací softvér FPWIN Pro7, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru spôsobiť pretečenie zásobníka a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.07.2023

CVE

CVE-2023-28728, CVE-2023-28729, CVE-2023-28730

Zasiahnuté systémy

Panasonic Control FPWIN Pro7 vo verzii staršej ako 7.7.0.0

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

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-192-03
https://industry.panasonic.eu/products/automation-devices-solutions/programmable-logic-controllers-plc/plc-software/programming-software-control-fpwin-pro

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

Identifikátor

Sensormatic Electronics iSTAR - bezpečnostná zraniteľnosť

Popis

Spoločnosť Sensormatic Electronics vydala bezpečnostnú aktualizáciu na svoj produkt iSTAR, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

11.07.2023

CVE

CVE-2023-3127

Zasiahnuté systémy

Sensormatic Electronics iSTAR Ultra vo verzii firmvéru staršej ako 6.9.2 CU01
Sensormatic Electronics iSTAR Ultra LT vo verzii firmvéru staršej ako 6.9.2 CU01
Sensormatic Electronics iSTAR Ultra G2 vo verzii firmvéru staršej ako 6.9.2 CU01
Sensormatic Electronics iSTAR Edge G2 vo verzii firmvéru staršej ako 6.9.2 CU01

Následky

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

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-192-02
https://nvd.nist.gov/vuln/detail/CVE-2023-3127
https://www.johnsoncontrols.com/-/media/jci/cyber-solutions/product-security-advisories/2023/jci-psa-2023-05.pdf?la=en&hash=C5E02BC753922BE0EE64194F44CFE8C981D2E428

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

Identifikátor

HPE Intelligent Provisioning - bezpečnostná zraniteľnosť

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostnú aktualizáciu na svoj produkt Intelligent Provisioning, ktorá opravuje 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

13.07.2023

CVE

CVE-2023-30906

Zasiahnuté systémy

Intelligent Provisioning pre Gen9 vo verzii staršej ako v2.87

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://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04486en_us