BEZPEČNOSTNÝ BULLETIN

Týždeň 21. 12. 2022 - 27. 12. 2022

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-970

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

Identifikátor

OpenStack - dve zero-day bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu OpenStack.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá na používateľa root a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepristupnenie služby.
Hoci výskumníci testovali verziu OpenStack aktuálnu ku dňu 9.8.2022, SK-CERT overil, že dané zraniteľnosti neboli odstránené ani vo verzii aktuálnej ku dňu 27.12.2022.

Dátum prvého zverejnenia varovania

20.12.2022

CVE

CVE-2022-38060, CVE-2022-38065

Zasiahnuté systémy

OpenStack git master 05194e7618

Následky

Eskalácia privilégií na používateľa root
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať.
Pre dočasnú mitigáciu odporúčame minimalizovať prístup používateľov na dotknuté systémy cez neprivilegované účty a tiež zaviesť detailný monitoring aktivít na OpenStack serveroch prostredníctvom nezávislého servera a vykonávať pravidelný audit týchto logov.
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://talosintelligence.com/vulnerability_reports/TALOS-2022-1589
https://talosintelligence.com/vulnerability_reports/TALOS-2022-1599
https://bugs.launchpad.net/oslo.privsep/+bug/1989008
https://opendev.org/openstack/openstack/commit/63c13c21441bb810a731b3169553ab8463da47e5

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

Identifikátor

D-Link DIR-882 - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach routera D-Link DIR-882.
Najzávažnejšia 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

25.12.2022

CVE

CVE-2022-46560, CVE-2022-46561, CVE-2022-46563, CVE-2022-46566, CVE-2022-46568

Zasiahnuté systémy

D-Link DIR-882 vo všetkých verziách firmvéru

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.

Zdroje

https://hackmd.io/@0dayResearch/ry55QVQvj
https://exchange.xforce.ibmcloud.com/vulnerabilities/242971
https://exchange.xforce.ibmcloud.com/vulnerabilities/242975
https://exchange.xforce.ibmcloud.com/vulnerabilities/242974
https://exchange.xforce.ibmcloud.com/vulnerabilities/242973
https://exchange.xforce.ibmcloud.com/vulnerabilities/242970
https://www.secureswitches.com/D-Link-EOL.asp

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Rockwell Automation Logix PLCs - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu na svoje portfólio PLC Logix, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.12.2022

CVE

CVE-2022-3157, CVE-2022-3166, CVE-2022-46670

Zasiahnuté systémy

For CompactLogix 5370 vo verzii staršej ako 33.013 alebo 34.011
Compact GuardLogix 5370 vo verzii staršej ako 33.013 alebo 34.011
ControlLogix 5570 vo verzii staršej ako 33.013 alebo 34.011
GuardLogix 5570 vo verzii staršej ako 33.013 alebo 34.011
ControlLogix 5570 vo verzii staršej ako 33.052 alebo 34.051
MicroLogix 1100 vo všetkých verziách
MicroLogix 1400 vo verziách starších ako 7.000 (vrátane)
MicroLogix 1400 B/C vo verziách starších ako 21.007 (vrátane)

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.
Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN).
Výrobca používateľom nepodporovaných Micrologix PLC odporúčajú prejsť na modely MicroLogix 800 alebo MicroLogix 850, ktoré nedisponujú komponentom web server.
Pre dočasnú mitigáciu výrobca odporúča znefunkčniť web server komponent a znefunkčniť HTTP/Port 802.

Zdroje

https://www.cisa.gov/uscert/ics/advisories/icsa-22-354-02
https://www.cisa.gov/uscert/ics/advisories/icsa-22-354-04

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

Identifikátor

NVIDIA - viacero bezpečnostných zraniteľností

Popis

Spoločnosť NVIDIA 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 pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.12.2022

CVE

-

Zasiahnuté systémy

SBIOS Firmware pre DGX A100 vo verzii staršej ako 1.18
BMC Firmware pre DGX A100 vo verzii staršej ako 00.19.07
SBIOS Firmware pre DGX Station A100 vo verzii staršej ako 10.16

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://nvidia.custhelp.com/app/answers/detail/a_id/5435

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

Identifikátor

Fuji Electric Tellus Lite V-Simulator - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Fuji Electric vydala bezpečnostnú aktualizáciu na svoj produkt Tellus Lite V-Simulator, 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

20.12.2022

CVE

CVE-2022-3085, CVE-2022-3087

Zasiahnuté systémy

Tellus Lite V-Simulator vo verzii staršej ako 4.0.15.0.

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN).
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/uscert/ics/advisories/icsa-22-354-01

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

Identifikátor

Omron CX-Programmer - bezpečnostná zraniteľnosť

Popis

Spoločnosť Omron vydala bezpečnostnú aktualizáciu na svoj programovací softvér CX-Programmer, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného CXP súboru získať prístup k citlivým údajom alebo vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

22.12.2022

CVE

CVE-2022-43509

Zasiahnuté systémy

Omron CX-Programmer vo verzii staršej ako 9.79

Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým informáciám

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace systémy a jednotky odporúčame prevádzkovať úplne oddelené od internetu.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Po odstránení zraniteľností, ktoré mohli spôsobiť vykonanie škodlivého kódu 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/uscert/ics/advisories/icsa-22-356-04

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

Identifikátor

Rockwell Automation Studio 5000 Logix Emulate - bezpečnostná zraniteľnosť

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu na svoj produkt Studio 5000 Logix Emulate, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom zabezpečení mechanizmov autentifikácie a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.12.2022

CVE

CVE-2022-3156

Zasiahnuté systémy

Studio 5000 Logix Emulate vo verzii staršej ako 34.00

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace systémy a jednotky odporúčame prevádzkovať úplne oddelené od internetu.
Po odstránení zraniteľností, ktoré mohli spôsobiť vykonanie škodlivého kódu 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/uscert/ics/advisories/icsa-22-356-02

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

Identifikátor

cURL libcurl - bezpečnostná zraniteľnosť

Popis

Vývojári knižnice libcurl vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky obísť HSTS check a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

21.12.2022

CVE

CVE-2022-43551

Zasiahnuté systémy

curl vo verzii staršej ako 7.87.0

Následky

Neoprávnená zmena v systéme

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nie sú založené na predmetnej knižnici v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu komponentov, od ktorých závisí Vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://curl.se/docs/CVE-2022-43551.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/242798

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

Identifikátor

Junos OS a Junos OS Evolved - bezpečnostná zraniteľnosť

Popis

Spoločnosť Juniper Networks vydala bezpečnostné aktualizácie na operačné systémy June OS a Junos OS Evolved, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom špeciálne vytvorenej BGP update správy spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

22.12.2022

CVE

CVE-2022-22184

Zasiahnuté systémy

Junos OS vo verzii staršej ako 22.3R1-S1, 22.3R2 a 22.4R1
Junos OS Evolved vo verzii staršej ako 22.3R1-S1-EVO, 22.3R2-EVO, a 22.4R1-EVO

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://supportportal.juniper.net/s/article/2022-12-Out-of-Cycle-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-A-BGP-session-will-flap-upon-receipt-of-a-specific-optional-transitive-attribute-in-version-22-3R1-CVE-2022-22184?language=en_US
https://nvd.nist.gov/vuln/detail/CVE-2022-22184

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

Identifikátor

OpenSSL - bezpečnostná zraniteľnosť

Popis

Vývojári knižnice OpenSSL vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného X.509 certifikátu spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.12.2022

CVE

CVE-2022-3996

Zasiahnuté systémy

OpenSSL vo verzii staršej ako 3.0.8

Následky

Zneprístupnenie služby

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy, SDK alebo moduly v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí Vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.

Zdroje

https://www.openssl.org/news/secadv/20221213.txt
https://nvd.nist.gov/vuln/detail/CVE-2022-3996
https://security.sios.jp/vulnerability/openssl-security-vulnerability-20221214/

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

Identifikátor

Mitsubishi Electric MELSEC a MELIPC - bezpečnostná zraniteľnosť

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostnú aktualizáciu na svoje produkty MELSEC iQ-R, iQ-L Series a MELIPC Series, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených packetov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

22.12.2022

CVE

CVE-2022-33324

Zasiahnuté systémy

MELSEC iQ-R Series R00/01/02CPU vo verzii staršej ako "33"
MELSEC iQ-R Series R04/08/16/32/120(EN)CPU vo verzii staršej ako "66"
MELSEC iQ-R Series R08/16/32/120SFCPU (všetky verzie)
MELSEC iQ-R Series R12CCPU-V (všetky verzie)
MELSEC iQ-L Series L04/08/16/32HCPU (všetky verzie)
MELIPC Series MI5122-VW (všetky verzie)

Následky

Zneprístupnenie služby

Odporúčania

Používateľom MELSEC iQ-R Series R00/01/02CPU a MELSEC iQ-R Series R04/08/16/32/120(EN)CPU odporúčame vykonať bezpečnostné aktualizácie.
Používateľom MELSEC iQ-R Series R08/16/32/120SFCPU, MELSEC iQ-R Series R12CCPU-V series L04/08/16/32HCPU a MELIPC Series MI5122-VW odporúčame postupovať podľa odporúčaní zverejnených na webstránke výrobcu na adrese https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-018_en.pdf

Zdroje

https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-018_en.pdf
https://www.cisa.gov/uscert/ics/advisories/icsa-22-356-03

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

Identifikátor

Priva TopControl Suite - bezpečnostná zraniteľnosť

Popis

Spoločnosť Priva vydala bezpečnostnú aktualizáciu na svoj produkt TopControl Suite, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom zabezpečení mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi dešifrovať prihlasovacie údaje k SSH a následne získať úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

22.12.2022

CVE

CVE-2022-3010

Zasiahnuté systémy

Priva TopControl Suite vo verzii staršej ako 8.7.8.0

Následky

Získanie úplnej kontroly nad systémom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace systémy a jednotky odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.cisa.gov/uscert/ics/advisories/icsa-22-356-01

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

Identifikátor

HPE Superdome Flex Server - bezpečnostná zraniteľnosť

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostné aktualizácie na produkty Superdome Flex Server a Superdome Flex 280 Server, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom injekcie špeciálne upravených príkazov spôsobiť narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.12.2022

CVE

CVE-2022-37933

Zasiahnuté systémy

HPE Superdome Flex Server vo verzii staršej ako 3.60.50
HPE Superdome Flex 280 Server vo verzii staršej ako 1.4.60

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Manažmentové rozhrania zariadení a serverov odporúčame nesprístupňovať z verejného Internetu. Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN).
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=hpesbhf04400en_us

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

Identifikátor

Delta Industrial Automation 4G Router DX-3021 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Delta Industrial Automation vydala bezpečnostnú aktualizáciu na svoj industriálny router DX-3021, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom injekcie špeciálne upravených príkazov spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.12.2022

CVE

CVE-2022-4616

Zasiahnuté systémy

DX-3021L9 vo verzii staršej ako V1.24

Následky

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.
Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.
Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN).

Zdroje

https://www.cisa.gov/uscert/ics/advisories/icsa-22-354-05

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.1
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

JSON5 - bezpečnostná zraniteľnosť

Popis

Vývojári knižnice JSON5 vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zneužitia prototype pollution zraniteľnosti vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.12.2022

CVE

CVE-2022-46175

Zasiahnuté systémy

JSON5 vo verzii staršej ako 2.2.2

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy, SDK alebo moduly v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí Vaša aplikácia, 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.

Zdroje

https://github.com/json5/json5/security/advisories/GHSA-9c47-m6qq-7p4h
https://nvd.nist.gov/vuln/detail/CVE-2022-46175