BEZPEČNOSTNÝ BULLETIN

Týždeň 27. 07. 2022 - 02. 08. 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-847

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

Identifikátor

Samba - viacero bezpečnostných zraniteľností

Popis

Vývojári open-source implementácie sieťového protokolu SMB Samba vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zneužitia chyby v Password Change Handler komponente eskalovať svoje privilégiá a získať úplnú kontrolu nad doménou.
Ostatné zraniteľnosti by útočníci mohli znežiť na zneprístupnenie služby a získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

27.07.2022

CVE

CVE-2022-2031, CVE-2022-32742, CVE-2022-32744, CVE-2022-32745, CVE-2022-32746

Zasiahnuté systémy

Samba vo verzii staršej ako 4.16.4

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.samba.org/samba/history/samba-4.16.4.html
https://nakedsecurity.sophos.com/2022/07/27/critical-samba-bug-could-let-anyone-become-domain-admin-patch-now/
https://www.samba.org/samba/security/CVE-2022-2031.html
https://www.samba.org/samba/security/CVE-2022-32742.html
https://www.samba.org/samba/security/CVE-2022-32744.html
https://www.samba.org/samba/security/CVE-2022-32745.html
https://www.samba.org/samba/security/CVE-2022-32746.html

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

Identifikátor

Mozilla produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Mozilla Foundation vydala bezpečnostné aktualizácie na produkty Mozilla Firefox a Firefox ESR, ktoré opravujú dve bezpečnostné zraniteľnosti.
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

26.07.2022

CVE

CVE-2022-2505, CVE-2022-36314, CVE-2022-36315, CVE-2022-36316, CVE-2022-36317, CVE-2022-36318, CVE-2022-36319, CVE-2022-36320

Zasiahnuté systémy

Mozilla Firefox vo verzii staršej ako 103
Firefox ESR vo verzii staršej ako 91.12

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
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 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.mozilla.org/en-US/security/advisories/mfsa2022-30/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-29/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-28/
https://exchange.xforce.ibmcloud.com/vulnerabilities/232060

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Moxa NPort 5110 - dve bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu MOXA NPort 5110 device server.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

26.07.2022

CVE

CVE-2022-2043, CVE-2022-2044

Zasiahnuté systémy

MOXA NPort 5110 device server vo verzii firmvéru 2.10

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje

https://www.cisa.gov/uscert/ics/advisories/icsa-22-207-04

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

Identifikátor

Cloudflare WARP Client - bezpečnostná zraniteľnosť

Popis

Spoločnosť Cloudflare vydala bezpečnostnú aktualizáciu na svoj produkt Cloudflare WARP Client, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky využívajúcej warp-cli príkazy obísť nastavenia Zero Trust politík a spôsobiť narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.07.2022

CVE

CVE-2022-2225

Zasiahnuté systémy

Cloudflare WARP Client (Windows) vo verzii staršej ako 2022.5.341.0
Cloudflare WARP Client (Linux) vo verzii staršej ako 2022.5.346
Cloudflare WARP Client (MacOS) vo verzii staršej ako 2022.5.227.0

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.

Zdroje

https://github.com/cloudflare/advisories/security/advisories/GHSA-cg88-vx48-976c
https://exchange.xforce.ibmcloud.com/vulnerabilities/232205

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

Identifikátor

LibreOffice - viacero bezpečnostných zraniteľností

Popis

Vývojári kancelárskeho balíka LibreOffice vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.07.2022

CVE

CVE-2022-26305, CVE-2022-26306, CVE-2022-26307

Zasiahnuté systémy

LibreOffice vo verzii staršej ako 7.2.7 alebo 7.3.2

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.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/231963
https://www.libreoffice.org/about-us/security/advisories/cve-2022-26305

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

Identifikátor

Honeywell Saia Burgess a Safety Manager - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktov Safety Manager a Saia Burgess PG5 PCD.
Najzávažnejšia bezpečnostná zraniteľnosť v produkte Saia Burgess PG5 PCD spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje neautentifikovanému útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente získať neoprávnený prístup do systému a následne spôsobiť narušenie dôvernosti, integrity a dostupnosti systému.
Najzávažnejšiu zraniteľnosť v produkte Safety Manager by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

26.07.2022

CVE

CVE-2022-30313, CVE-2022-30314, CVE-2022-30315, CVE-2022-30316, CVE-2022-30319, CVE-2022-30320

Zasiahnuté systémy

Saia Burgess PG5 PCD - všetky verzie
Safety Manager - všetky verzie

Následky

Neoprávnený prístup do systému
Vykonanie škodlivého kódu a narušenie dôvernosti, integrity a dostupnosti systému.

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov. Do vydania bezpečnostných aktualizácií odporúčame postupovať podľa odporúčaní spoločnosti Honeywell, ktoré môžete nájsť na odkazoch v časti Zdroje.
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/uscert/ics/advisories/icsa-22-207-03
https://www.cisa.gov/uscert/ics/advisories/icsa-22-207-02

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

Identifikátor

Inductive Automation Ignition - bezpečnostná zraniteľnosť

Popis

Spoločnosť Inductive Automation vydala bezpečnostnú aktualizáciu na svoj produkt Ignition, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zaslania špeciálne vytvoreného XML dokumentu spôsobiť narušenie dôvernosti a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.07.2022

CVE

CVE-2022-1704

Zasiahnuté systémy

Inductive Automation Ignition vo verzii staršej ako 8.1.9
Inductive Automation Ignition vo verzii staršej ako v7.9.21

Následky

Narušenie dôvernosti 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/uscert/ics/advisories/icsa-22-207-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.4
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Dahua IP kamery - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Dahua vydala bezpečnostnú aktualizáciu na vybrané modely svojich IP kamier, ktorá opravuje viacero bezpečnostných zraniteľností v implementácii ONVIF (Open Network Video Interface Forum) štandardu.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať úplnú kontrolu nad zariadením a následne spôsobiť narušenie dôvernosti a integrity systému.

Dátum prvého zverejnenia varovania

28.07.2022

CVE

CVE-2022-30560, CVE-2022-30561, CVE-2022-30562, CVE-2022-30563

Zasiahnuté systémy

Dahua ASI7XXX vo verzii staršej ako v1.000.0000009.0.R.220620
Dahua IPC-HDBW2XXX vo verzii staršej ako v2.820.0000000.48.R.220614
Dahua IPC-HX2XX vo verzii staršej ako v2.820.0000000.48.R.220614

Následky

Neoprávnený prístup do systému
Úplné narušenie dôvernosti a integrity 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.nozominetworks.com/blog/vulnerability-in-dahua-s-onvif-implementation-threatens-ip-camera-security/
https://thehackernews.com/2022/07/dahua-ip-camera-vulnerability-could-let.html
https://www.dahuasecurity.com/support/cybersecurity/details/1017