BEZPEČNOSTNÝ BULLETIN

Týždeň 02. 03. 2022 - 08. 03. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	IPCOMM ipDIO produkt - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	PJSIP knižnica - viacero bezpečnostných zraniteľností	Vysoká	**8.1**
03.	BD Viper LT produkt - dve bezpečnostné zraniteľnosti	Vysoká	**8.0**
04.	Fortinet FortiAP-C - bezpečnostná zraniteľnosť	Vysoká	**7.8**
05.	TerraMaster TOS - bezpečnostná zraniteľnosť	Vysoká	**7.5**
06.	NetApp StorageGRID produkt - bezpečnostná zraniteľnosť	Vysoká	**7.5**

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-700

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

Identifikátor

IPCOMM ipDIO produkt - viacero bezpečnostných zraniteľností

Popis

Spoločnosť IPCOMM vydala bezpečnostnú aktualizáciu na produkt ipDIO, ktorá opravuje viacero bezpečnostných zraniteľností. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom povrhnutia špeciálne vytvoreného skriptu, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.03.2022

CVE

CVE-2022-21146, CVE-2022-22765, CVE-2022-22985, CVE-2022-24432, CVE-2022-24915

Zasiahnuté systémy

ipDIO 3.9 2016/04/18 / IPDIO SW 3.9 (všetky verzie - ukončená podpora)

Následky

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

Odporúčania

Vzhľadom k tomu, že produkt už nie je udržiavaný, výrobca odporúča prejsť na produkt ip4Cloud device 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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-22-062-01

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

Identifikátor

PJSIP knižnica - viacero bezpečnostných zraniteľností

Popis

Vývojári knižnice PJSIP vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.03.2022

CVE

CVE-2021-43299, CVE-2021-43300, CVE-2021-43301, CVE-2021-43302, CVE-2021-43303

Zasiahnuté systémy

PJSIP vo verzii staršej ako 2.12

Následky

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

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://jfrog.com/blog/jfrog-discloses-5-memory-corruption-vulnerabilities-in-pjsip-a-popular-multimedia-library/
https://threatpost.com/rce-bugs-whatsapp-popular-voip-apps-patch-now/178719/
https://thehackernews.com/2022/03/critical-bugs-reported-in-popular-open.html

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

Identifikátor

BD Viper LT produkt - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Becton, Dickinson and Company (BD) vydala bezpečnostnú aktualizáciu na produkt Viper LT, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

04.03.2022

CVE

CVE-2022-22765, CVE-2022-22766

Zasiahnuté systémy

BD Viper LT system vo verzii staršej ako 4.80

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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsma-22-062-02
https://us-cert.cisa.gov/ics/advisories/icsma-22-062-01

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

Identifikátor

Fortinet FortiAP-C - bezpečnostná zraniteľnosť

Popis

Spoločnosť Fortinet vydala bezpečnostnú aktualizáciu na produkt FortiAP-C, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.03.2022

CVE

CVE-2022-22301

Zasiahnuté systémy

Fortinet FortiAP-C vo verzii staršej ako 5.4.4

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 lokálne 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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://www.fortiguard.com/psirt/FG-IR-21-227
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22301
https://exchange.xforce.ibmcloud.com/vulnerabilities/220833

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

Identifikátor

TerraMaster TOS - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja TerraMaster TOS vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

07.03.2022

CVE

CVE-2022-24990

Zasiahnuté systémy

TerraMaster TOS vo verzii staršej ako 4.2.31

Následky

Neoprávnený prístup k citlivým údajom

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://octagon.net/blog/2022/03/07/cve-2022-24990-terrmaster-tos-unauthenticated-remote-command-execution-via-php-object-instantiation/
https://www.terra-master.com/global/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24990
https://exchange.xforce.ibmcloud.com/vulnerabilities/221114

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

Identifikátor

NetApp StorageGRID produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť NetApp vydala bezpečnostnú aktualizáciu na produkt StorageGRID, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

03.03.2022

CVE

CVE-2022-23233

Zasiahnuté systémy

NetApp StorageGRID vo verzii staršej ako 11.6.0

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://security.netapp.com/advisory/NTAP-20220303-0010/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23233
https://exchange.xforce.ibmcloud.com/vulnerabilities/221085