BEZPEČNOSTNÝ BULLETIN

Týždeň 20. 04. 2022 - 26. 04. 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-743

BEZPEČNOSTNÝ BULLETIN

Týždeň 20. 04. 2022 - 26. 04. 2022

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

Identifikátor

Delta Electronics ASDA-Soft produkt - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na produkt ASDA-Soft, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom povrhnutia špeciálne vytvorenej webovej stránky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.04.2022

CVE

CVE-2022-1402, CVE-2022-1403

Zasiahnuté systémy

ASDA-Soft vo verzii staršej ako v5.5.0.0

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 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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
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/icsa-22-111-01

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

Identifikátor

Linux Kernel - bezpečnostná zraniteľnosť

Popis

Vývojári jadra operačného systému Linux vydali bezpečnostnú aktualizáciu svojho produktu, 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 vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.04.2022

CVE

CVE-2022-29582

Zasiahnuté systémy

Linux Kernel vo verzii staršej ako 5.17.3

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

Zdroje

https://seclists.org/oss-sec/2022/q2/54
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=e677edbcabee849bfdd43f1602bccbecf736a646
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29582
https://exchange.xforce.ibmcloud.com/vulnerabilities/225034

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

Identifikátor

Amazon AWS amazon-ssm-agent - bezpečnostná zraniteľnosť

Popis

Spoločnosť Amazon vydala bezpečnostnú aktualizáciu na produkt AWS amazon-ssm-agent, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne vytvorenej požiadavky, eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.04.2022

CVE

CVE-2022-29527

Zasiahnuté systémy

Amazon AWS amazon-ssm-agent vo verzii staršej ako 3.1.1208.0

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 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://bugzilla.suse.com/show_bug.cgi?id=1196556
https://github.com/aws/amazon-ssm-agent/commit/0fe8ae99b2ff25649c7b86d3bc05fc037400aca7
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29527
https://exchange.xforce.ibmcloud.com/vulnerabilities/224878

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

Identifikátor

Cisco produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje dve bezpečnostné zraniteľnosti. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.04.2022

CVE

CVE-2022-20685, CVE-2022-20783

Zasiahnuté systémy

Cisco RoomOS Software vo verzii staršej ako RoomOS January 2022
Cisco TelePresence Collaboration Endpoint Software vo verzii staršej ako 9.15.10.8
Cisco TelePresence Collaboration Endpoint Software vo verzii staršej ako 10.11.2.2
Cisco FTD and FirePOWER Services vo verzii staršej ako 6.4.0.13
Cisco FTD and FirePOWER Services vo verzii staršej ako 6.6.5.1
Cisco FTD and FirePOWER Services vo verzii staršej ako 7.0.1
Cisco Cyber Vision vo verzii staršej ako 4.0.2
Cisco UTD vo verzii staršej ako 16.12.7
Cisco UTD vo verzii staršej ako 17.3.5
Cisco UTD vo verzii staršej ako 17.6.2
Cisco Snort vo verzii staršej ako 2.9.19
Cisco Snort vo verzii staršej ako 3.1.11.0

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ce-roomos-dos-c65x2Qf2
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20783
https://exchange.xforce.ibmcloud.com/vulnerabilities/224850
https://thehackernews.com/2022/04/researchers-detail-bug-that-could.html
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-dos-9D3hJLuj

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

Identifikátor

ASUS WebStorage pre Android - bezpečnostná zraniteľnosť

Popis

Spoločnosť ASUS vydala bezpečnostnú aktualizáciu na produkt WebStorage pre Android, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v existencii zabudovaného API tokenu a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

22.04.2022

CVE

CVE-2022-26672

Zasiahnuté systémy

ASUS WebStorage pre Android vo verzii staršej ako 3.10.2

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.

Zdroje

https://www.twcert.org.tw/tw/cp-132-6041-7bd67-1.html
https://www.asus.com/us/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26672
https://exchange.xforce.ibmcloud.com/vulnerabilities/225047