BEZPEČNOSTNÝ BULLETIN

Týždeň 20. 10. 2021 - 26. 10. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Delta Electronics DIALink produkt - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	Schneider Electric ConneXium Network Manager - bezpečnostná zraniteľnosť	Vysoká	**7.8**
03.	eLabFTW produkt - bezpečnostná zraniteľnosť	Vysoká	**7.5**
04.	QNAP NAS Media Streaming add-on - bezpečnostná zraniteľnosť	Vysoká	**7.3**
05.	Rasa X produkt - bezpečnostná zraniteľnosť	Vysoká	**7.3**
06.	WP Mailster plugin pre WordPress - bezpečnostná zraniteľnosť	Vysoká	**7.2**

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:
01439/2020/SK-CERT-597

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

Identifikátor

Delta Electronics DIALink produkt - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu DIALink od spoločnosti Delta Electronics.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.10.2021

CVE

CVE-2021-38403, CVE-2021-38407, CVE-2021-38411, CVE-2021-38416, CVE-2021-38418, CVE-2021-38420, CVE-2021-38422, CVE-2021-38424, CVE-2021-38428, CVE-2021-38488

Zasiahnuté systémy

DIALink vo verzii staršej ako 1.2.4.0 (vrátane)

Následky

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

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-294-02

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

Identifikátor

Schneider Electric ConneXium Network Manager - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu ConneXium Network Manager Software od spoločnosti Schneider Electric.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom povrhnutia špeciálne vytvorenej webovej stránky, eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.10.2021

CVE

CVE-2021-22801

Zasiahnuté systémy

ConneXium Network Manager všetky verzie

Následky

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

Odporúčania

Administrátorom a používateľom odporúča výrobca nainštalovať CNM Alarms Disabler Tool a postupovať podľa pokynov uvedených na webovej stránke:
https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-285-02
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.
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-285-02
https://us-cert.cisa.gov/ics/advisories/icsa-21-287-01

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

Identifikátor

eLabFTW produkt - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja eLabFTW 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

22.10.2021

CVE

CVE-2021-41171

Zasiahnuté systémy

eLabFTW vo verzii staršej ako 4.1.0

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://github.com/elabftw/elabftw/security/advisories/GHSA-q67h-5pc3-g6jv
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41171
https://exchange.xforce.ibmcloud.com/vulnerabilities/211901

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

Identifikátor

QNAP NAS Media Streaming add-on - bezpečnostná zraniteľnosť

Popis

Spoločnosť QNAP vydala bezpečnostnú aktualizáciu na produkt NAS Media Streaming add-on, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

22.10.2021

CVE

CVE-2021-34362

Zasiahnuté systémy

QTS 5.0.0 s Media Streaming add-on vo verzii staršej ako 500.0.0.3 (2021/08/20)
QTS 4.5.4 s Media Streaming add-on vo verzii staršej ako 500.0.0.3 (2021/08/20)
QTS 4.3.6 s Media Streaming add-on vo verzii staršej ako 430.1.8.12 (2021/08/20)
QTS 4.3.3 s Media Streaming add-on vo verzii staršej ako 430.1.8.12 (2021/09/29)
QuTS hero h5.0.0 s Media Streaming add-on vo verzii staršej ako 500.0.0.3 (2021/08/20)

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.qnap.com/en/security-advisory/qsa-21-44
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34362
https://exchange.xforce.ibmcloud.com/vulnerabilities/211891

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

Identifikátor

Rasa X produkt - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja Rasa X vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom povrhnutia špeciálne vytvorených súborov, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

21.10.2021

CVE

CVE-2021-42556

Zasiahnuté systémy

Rasa X vo verzii staršej ako 0.42.4

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

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.

Zdroje

https://github.com/RasaHQ/rasa-x-security-advisories/security/advisories/GHSA-vp2h-j6px-56rc
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42556
https://exchange.xforce.ibmcloud.com/vulnerabilities/211920

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

Identifikátor

WP Mailster plugin pre WordPress - bezpečnostná zraniteľnosť

Popis

Vývojári pluginu Mailster pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom injekcie škodlivého skriptu, získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

21.10.2021

CVE

CVE-2021-28975

Zasiahnuté systémy

WP Mailster vo verzii staršej ako 1.6.21

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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.compass-security.com/fileadmin/Research/Advisories/2021-18_CSNC-2021-018-WPMailster_XSS_CSRF.txt
https://wordpress.org/plugins/wp-mailster/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28975
https://exchange.xforce.ibmcloud.com/vulnerabilities/211883