BEZPEČNOSTNÝ BULLETIN

Týždeň 08. 12. 2021 - 14. 12. 2021

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:
01439/2020/SK-CERT-635

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

Identifikátor

Advantech R-SeeNet produkt - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Advantech vydala bezpečnostnú aktualizáciu na produkt R-SeeNet, ktorá opravuje viacero bezpečnostných zraniteľností. Najzávažnejšia 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

14.12.2021

CVE

CVE-2021-21910, CVE-2021-21911, CVE-2021-21912, CVE-2021-21915, CVE-2021-21916, CVE-2021-21917, CVE-2021-21918, CVE-2021-21919, CVE-2021-21920, CVE-2021-21921, CVE-2021-21922, CVE-2021-21923, CVE-2021-21924, CVE-2021-21925, CVE-2021-21926, CVE-2021-21927, CVE-2021-21928, CVE-2021-21929, CVE-2021-21930, CVE-2021-21931, CVE-2021-21932, CVE-2021-21933, CVE-2021-21934, CVE-2021-21935, CVE-2021-21936, CVE-2021-21937

Zasiahnuté systémy

R-SeeNet vo verzii staršej ako 2.4.17

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).
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-348-01

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

Identifikátor

Hillrom Welch Allyn Cardio produkt - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Welch Allyn Cardio od spoločnosti Hillrom.
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

09.12.2021

CVE

CVE-2021-43935

Zasiahnuté systémy

Welch Allyn Q-Stress Cardiac Stress Testing System vo verzii staršej ako 6.3.1 (vrátane)
Welch Allyn X-Scribe Cardiac Stress Testing System vo verzii staršej ako 6.3.1 (vrátane)
Welch Allyn Diagnostic Cardiology Suite vo verzii staršej ako 2.1.0 (vrátane)
Welch Allyn Vision Express vo verzii staršej ako 6.4.0 (vrátane)
Welch Allyn H-Scribe Holter Analysis System vo verzii staršej ako 6.4.0 (vrátane)
Welch Allyn R-Scribe Resting ECG System vo verzii staršej ako 7.0.0 (vrátane)
Welch Allyn Connex Cardio vo verzii staršej ako 1.1.1 (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.
Zdravotnícke zariadenia a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsma-21-343-01
https://portswigger.net/daily-swig/zero-day-vulnerability-in-hillrom-cardiology-devices-could-allow-attackers-full-control

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

Identifikátor

WECON LeviStudioU - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu LeviStudioU od spoločnosti WECON.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.12.2021

CVE

CVE-2021-43983

Zasiahnuté systémy

LeviStudioU vo verzii staršej ako 2019-09-21 (vrátane)

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.
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-21-343-02

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

Identifikátor

Apple iOS a iPadOS - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Apple vydala bezpečnostnú aktualizáciu na produkty iOS a iPadOS, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom povrhnutia špeciálne vytvorených súborov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.12.2021

CVE

CVE-2021-30767, CVE-2021-30926, CVE-2021-30927, CVE-2021-30929, CVE-2021-30932, CVE-2021-30934, CVE-2021-30936, CVE-2021-30937, CVE-2021-30939, CVE-2021-30940, CVE-2021-30941, CVE-2021-30942, CVE-2021-30945, CVE-2021-30946, CVE-2021-30947, CVE-2021-30948, CVE-2021-30949, CVE-2021-30951, CVE-2021-30952, CVE-2021-30953, CVE-2021-30954, CVE-2021-30955, CVE-2021-30957, CVE-2021-30958, CVE-2021-30960, CVE-2021-30964, CVE-2021-30966, CVE-2021-30967, CVE-2021-30968, CVE-2021-30971, CVE-2021-30973, CVE-2021-30979, CVE-2021-30980, CVE-2021-30983, CVE-2021-30984, CVE-2021-30985, CVE-2021-30988, CVE-2021-30991, CVE-2021-30992, CVE-2021-30993, CVE-2021-30995, CVE-2021-30996

Zasiahnuté systémy

Apple iOS vo verzii staršej ako 15.2
Apple iPadOS vo verzii staršej ako 15.2

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.
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).

Zdroje
https://support.apple.com/en-us/HT212976
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30957
https://exchange.xforce.ibmcloud.com/vulnerabilities/215080
https://thehackernews.com/2021/12/latest-apple-ios-update-patches-remote.html

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

Identifikátor

Hitachi Energy GMS600, PWC600 a Relion produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Hitachi Energy vydala bezpečnostné aktualizácie na produkty GMS600, PWC600 a Relion, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.12.2021

CVE

CVE-2021-35534

Zasiahnuté systémy

GMS600 vo verzii 1.2.0
GMS600 vo verzii 1.3.0
GMS600 vo verzii 1.3.1.0
PWC600 vo verzii 1.1.0.0
PWC600 vo verzii 1.1.0.1
PWC600 vo verzii 1.0.1.0
PWC600 vo verzii 1.0.1.1
PWC600 vo verzii 1.0.1.3
PWC600 vo verzii 1.0.1.4
Relion 670 vo verzii staršej ako 2.2.3.5
Relion 670/650/SAM600-IO vo verzii staršej ako 2.2.5.2
Relion 650 vo verzii staršej ako 1.3.0.8
Relion 650 vo verzii staršej ako 1.3

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje
https://us-cert.cisa.gov/ics/advisories/icsa-21-343-01 https://search.abb.com/library/Download.aspx?DocumentID=8DBD000060&LanguageCode=en&DocumentPartId=&Action=Launch

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

Identifikátor

GitLab - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja GitLab 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 zasielania špeciálne vytvorenej požiadavky, eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajomvykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

12.12.2021

CVE

CVE-2021-39944

Zasiahnuté systémy

GitLab vo verzii staršej ako 14.3.6
GitLab vo verzii staršej ako 14.4.4
GitLab vo verzii staršej ako 14.5.2

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Eskalácia privilégií

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://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39944.json
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39944
https://exchange.xforce.ibmcloud.com/vulnerabilities/215167