BEZPEČNOSTNÝ BULLETIN

Týždeň 01. 12. 2021 - 07. 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-628

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SolarWinds Serv-U File Server - bezpečnostná zraniteľnosť

Popis

Spoločnosť SolarWinds vydala bezpečnostnú aktualizáciu na produk Serv-U File Server, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.12.2021

CVE

CVE-2021-35245

Zasiahnuté systémy

SolarWinds Serv-U File Server vo verzii staršej ako 15.2.5

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.

Zdroje

https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_15-2-5_release_notes.htm
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35245
https://exchange.xforce.ibmcloud.com/vulnerabilities/214567

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-628

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.3**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Sensormatic Electronics Entrapass produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Sensormatic Electronics vydala bezpečnostnú aktualizáciu na produkt Entrapass, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

02.12.2021

CVE

CVE-2021-36198

Zasiahnuté systémy

Entrapass vo verzii staršej ako 8.40

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

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-336-02
https://www.johnsoncontrols.com/-/media/jci/cyber-solutions/product-security-advisories/2021/jci-psa-2021-22.pdf

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

Identifikátor

Xylem Aanderaa GeoView produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Xylem vydala bezpečnostnú aktualizáciu na produkt Aanderaa GeoView, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

30.11.2021

CVE

CVE-2021-41063

Zasiahnuté systémy

AADI GeoView Webservice vo verzii staršej ako v2.1.3

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

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-334-01

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

Identifikátor

Hitachi Energy RTU500 a Relion produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Hitachi Energy vydala bezpečnostnú aktualizáciu na produkty RTU500 a Relion, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených paketov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.12.2021

CVE

CVE-2021-35533, CVE-2021-35535

Zasiahnuté systémy

RTU500 s firmware vo verzii staršej ako 12.6.5.0
RTU500 s firmware vo verzii staršej ako 12.7.*
RTU500 s firmware vo verzii staršej ako 13.2.*
Relion 670/650 vo verzii staršej ako 2.2.5
Relion 670/650/SAM600-IO vo verzii staršej ako 2.2.5

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.
Výrobca odporúča pre produkt RTU500 vypnúť funkciu BCI IEC 60870-5-104 v prípade, že sa nepoužíva.
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-21-336-04 https://us-cert.cisa.gov/ics/advisories/icsa-21-336-05 https://search.abb.com/library/Download.aspx?utm_campaign=2021.11_5282_Cybersecurity%20Advisory&utm_content=2021.11_5282_Cybersecurity%20Advisory&utm_medium=email&utm_source=Eloqua&DocumentID=8DBD000063&LanguageCode=en&DocumentPartId=&Action=Launch&elqTrackId=af857fe4745f4180a42aa0778f76b1b9&elq=38e0453737cf4db980910db6ef0c9e36&elqaid=3812&elqat=1&elqCampaignId=3243

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

Identifikátor

Delta Electronics CNCSoft produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na produkt CNCSoft, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.11.2021

CVE

CVE-2021-43982

Zasiahnuté systémy

CNCSoft vo verzii staršej ako 1.01.30

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-21-334-03

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

Identifikátor

Mitsubishi Electric MELSEC a MELIPC produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostnú aktualizáciu na produkty MELSEC a MELIPC, ktorá opravuje viacero bezpečnostných zraniteľností. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

30.11.2021

CVE

CVE-2021-20609, CVE-2021-20610, CVE-2021-20611

Zasiahnuté systémy

MELSEC iQ-R Series R00/01/02CPU s firmware vo verzii staršej ako 25
MELSEC iQ-R Series R04/08/16/32/120(EN)CPU s firmware vo verzii staršej ako 58
MELSEC iQ-R Series R08/16/32/120SFCPU všetky verzie
MELSEC iQ-R Series R08/16/32/120PCPU s firmware vo verzii staršej ako 30
MELSEC iQ-R Series R08/16/32/120PSFCPU všetky verzie
MELSEC iQ-R Series R16/32/64MTCPU všetky verzie
MELSEC iQ-R Series R12CCPU-V všetky verzie
MELSEC Q Series Q03/04/06/13/26UDVCPU s firmware vo verzii staršej ako 23072
MELSEC Q Series Q04/06/13/26UDPVCPU s firmware vo verzii staršej ako 23072
MELSEC Q Series Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU všetky verzie
MELSEC Q Series Q12DCCPU-V, Q24DHCCPU-V(G), Q24/26DHCCPU-LS všetky verzie
MELSEC Q Series MR-MQ100 všetky verzie
MELSEC Q Series Q172/173DCPU-S1, Q172/172DSCPU všetky verzie
MELSEC Q Series Q170MCPU, Q170MSCPU(-S1) všetky verzie
MELSEC L Series L02/06/26CPU(-P), L26CPU-(P)BT všetky verzie
MELIPC Series MI5122-VW všetky verzie

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-334-02
https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf