BEZPEČNOSTNÝ BULLETIN

Týždeň 15. 09. 2021 - 21. 09. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

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

Identifikátor

Siemens RUGGEDCOM ROX produkt - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Siemens vydala bezpečnostnú aktualizáciu na produkt RUGGEDCOM ROX, ktorá opravuje viacero bezpečnostných zraniteľností. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, 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

21.09.2021

CVE

CVE-2021-37173, CVE-2021-37174, CVE-2021-37175

Zasiahnuté systémy

RUGGEDCOM ROX MX5000 vo verzii staršej ako v2.14.1
RUGGEDCOM ROX RX1400 vo verzii staršej ako v2.14.1
RUGGEDCOM ROX RX1500 vo verzii staršej ako v2.14.1
RUGGEDCOM ROX RX1501 vo verzii staršej ako v2.14.1
RUGGEDCOM ROX RX1510 vo verzii staršej ako v2.14.1
RUGGEDCOM ROX RX1511 vo verzii staršej ako v2.14.1
RUGGEDCOM ROX RX1512 vo verzii staršej ako v2.14.1
RUGGEDCOM ROX RX1524 vo verzii staršej ako v2.14.1
RUGGEDCOM ROX RX1536 vo verzii staršej ako v2.14.1
RUGGEDCOM ROX RX5000 vo verzii staršej ako v2.14.1

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://cert-portal.siemens.com/productcert/pdf/ssa-150692.pdf
https://us-cert.cisa.gov/ics/advisories/icsa-21-259-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Sensormatic Electronics KT-1 produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Sensormatic Electronics vydala bezpečnostnú aktualizáciu na produkt KT-1, 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

16.09.2021

CVE

CVE-2021-27662

Zasiahnuté systémy

KT-1 controller vo verzii staršej ako 3.04

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-21-257-02-0
https://www.johnsoncontrols.com/cyber-solutions/security-advisories

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

Identifikátor

Palo Alto Networks Cortex XSOAR a PAN-OS - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Palo Alto Networks vydala bezpečnostné aktualizácie na produkty Cortex XSOAR a PAN-OS, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.09.2021

CVE

CVE-2021-3051, CVE-2021-3052

Zasiahnuté systémy

Cortex XSOAR 6.2.0 vo verzii staršej ako 1578666
Cortex XSOAR 6.1.0 vo verzii staršej ako 1578663
Cortex XSOAR 5.5.0 vo verzii staršej ako 1578677
PAN-OS vo verzii staršej ako 10.1
PAN-OS vo verzii staršej ako 10.0.2
PAN-OS vo verzii staršej ako 9.1.10
PAN-OS vo verzii staršej ako 9.0.14
PAN-OS vo verzii staršej ako 8.1.20

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://security.paloaltonetworks.com/CVE-2021-3051
https://security.paloaltonetworks.com/CVE-2021-3052

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

Identifikátor

Schneider Electric produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Schneider Electric vydala bezpečnostné aktualizácie na produkty EcoStruxure Control Expert, EcoStruxure Process Expert, SCADAPack RemoteConnect for x70, ktoré opravujú bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom povrhnutia špeciálne vytvoreného súboru, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.09.2021

CVE

CVE-2021-22797

Zasiahnuté systémy

EcoStruxure Control Expert všetky verzie
EcoStruxure Process Expert všetky verzie
SCADAPack RemoteConnect pre x70 všetky verzie

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.
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-2021-257-01
https://us-cert.cisa.gov/ics/advisories/icsa-21-259-02

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.4**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Mitmproxy - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja mitmproxy 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 a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

16.09.2021

CVE

CVE-2021-39214

Zasiahnuté systémy

mitmproxy vo verzii staršej ako 7.0.3

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.

Zdroje

https://github.com/mitmproxy/mitmproxy/security/advisories/GHSA-22gh-3r9q-xf38
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39214
https://exchange.xforce.ibmcloud.com/vulnerabilities/209540

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.4**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache HTTP Server - bezpečnostná zraniteľnosť

Popis

Organizácia Apache vydala bezpečnostnú aktualizáciu na produkt Apache HTTP Server, 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 a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

16.09.2021

CVE

CVE-2021-40438

Zasiahnuté systémy

Apache HTTP Server 2.4.49

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

http://httpd.apache.org/security/vulnerabilities_24.html
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40438
https://exchange.xforce.ibmcloud.com/vulnerabilities/209526

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-557