BEZPEČNOSTNÝ BULLETIN

Týždeň 12. 05. 2021 - 18. 05. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Qualcomm Mobile Station Modem Interface - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	Rockwell Automation Connected Components Workbench - bezpečnostné zraniteľnosti	Vysoká	**8.6**
03.	SonicWall Email Security Virtual Appliance - bezpečnostná zraniteľnosť	Vysoká	**8.4**
04.	SAP NetWeaver AS ABAP produkt - bezpečnostná zraniteľnosť	Vysoká	**8.2**
05.	Wi-Fi zariadenia - viacero bezpečnostných zraniteľností	Vysoká	**8.0**
06.	Citrix Workspace App pre Windows - bezpečnostná zraniteľnosť	Vysoká	**7.8**
07.	McAfee Total Protection - dve bezpečnostné zraniteľnosti	Vysoká	**7.8**
08.	Omron CX-One CX-Server produkt - bezpečnostná zraniteľnosť	Vysoká	**7.8**
09.	Johnson Controls Sensormatic Tyco AI - bezpečnostná zraniteľnosť	Vysoká	**7.8**
10.	Schneider Electric Modicon M241 a M251 - bezpečnostná zraniteľnosť	Vysoká	**7.5**
11.	OPC UA Servers - viacero bezpečnostných zraniteľností	Vysoká	**7.5**
12.	Mitsubishi Electric GOT a Tension Controller produkty - bezpečnostná zraniteľnosť	Stredná	**5.9**

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-422

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

Identifikátor

Qualcomm Mobile Station Modem Interface - bezpečnostná zraniteľnosť

Popis

Spoločnosť Qualcomm vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré obsahujú čipy Qualcomm's Mobile Station Modem (MSM).
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej aplikácie, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.05.2021

CVE

CVE-2020-11292

Zasiahnuté systémy

Všetky zariadenia obsahujujúce Qualcomm's Mobile Station Modem (MSM) chips vo verzii staršej ako upd 7.12.2020
Presnú specifikáciu jednotlivých zasiahnutých produktov nájdete na webovej adrese:
https://www.qualcomm.com/company/product-security/bulletins/december-2020-security-bulletin

Následky

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

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.
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.

Zdroje

https://research.checkpoint.com/2021/security-probe-of-qualcomm-msm/
https://www.qualcomm.com/company/product-security/bulletins/december-2020-security-bulletin
https://threatpost.com/qualcomm-chip-bug-android-eavesdropping/165934/

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

Identifikátor

Rockwell Automation Connected Components Workbench - bezpečnostné zraniteľnosti

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu svojho produktu Connected Components Workbench, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.05.2021

CVE

CVE-2021-27471, CVE-2021-27473, CVE-2021-27475

Zasiahnuté systémy

Rockwell Automation Connected Components Workbench vo verzii staršej ako 13.00.00

Následky

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

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.
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.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-133-01

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

Identifikátor

SonicWall Email Security Virtual Appliance - bezpečnostná zraniteľnosť

Popis

Spoločnosť SonicWall vydala bezpečnostnú aktualizáciu na svoj produkt Email Security Virtual Appliance, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňuje lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá, získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

13.05.2021

CVE

CVE-2021-20025

Zasiahnuté systémy

SonicWall Email Security Virtual Appliance vo verzii staršej ako 10.0.10

Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0012
https://exchange.xforce.ibmcloud.com/vulnerabilities/201842

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

Identifikátor

SAP NetWeaver AS ABAP produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť SAP vydala bezpečnostnú aktualizáciu na svoj produkt NetWeaver AS ABAP, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, 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

11.05.2021

CVE

CVE-2021-27611

Zasiahnuté systémy

SAP NetWeaver AS ABAP vo verzii 700
SAP NetWeaver AS ABAP vo verzii 701
SAP NetWeaver AS ABAP vo verzii 702
SAP NetWeaver AS ABAP vo verzii 730
SAP NetWeaver AS ABAP vo verzii 731

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

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

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.

Zdroje

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=576094655
https://exchange.xforce.ibmcloud.com/vulnerabilities/201717
https://nvd.nist.gov/vuln/detail/CVE-2021-27611

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.0
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Wi-Fi zariadenia - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o kritických zraniteľnostiach FragAttacks, ktoré zasahujú zariadenia komunikujúce prostredníctvom Wi-Fi.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom zasielania špeciálne upravených paketov získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.
Na uvedené zraniteľnosti je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

12.05.2021

CVE

CVE-2020-24586, CVE-2020-24587, CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26142, CVE-2020-26143, CVE-2020-26144, CVE-2020-26145, CVE-2020-26146, CVE-2020-26147

Zasiahnuté systémy

Všetky Wi-Fi bezpečnostné protokoly (WEP,WPA,WPA2,WPA3)
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na webovej adrese:
https://www.icasi.org/aggregation-fragmentation-attacks-against-wifi/

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

Zdroje
https://www.fragattacks.com/ https://www.wi-fi.org/security-update-fragmentation https://www.icasi.org/aggregation-fragmentation-attacks-against-wifi/ https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wifi-faf-22epcEWu https://thehackernews.com/2021/05/nearly-all-wifi-devices-are-vulnerable.html https://threatpost.com/fragattacks-wifi-bugs-millions-devices/166080/ https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-wi-fi-enabled-devices-could-allow-for-data-exfiltration_2021-068/ https://www.bleepingcomputer.com/news/security/all-wi-fi-devices-impacted-by-new-fragattacks-vulnerabilities/ https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

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

Identifikátor

Citrix Workspace App pre Windows - bezpečnostná zraniteľnosť

Popis

Spoločnosť Citrix vydala bezpečnostnú aktualizáciu na svoj produkt Workspace App pre Windows, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.05.2021

CVE

CVE-2021-22907

Zasiahnuté systémy

Citrix Workspace app vo verzii staršej ako 21.5.0.48 (2105)

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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.

Zdroje

https://support.citrix.com/article/CTX307794
https://exchange.xforce.ibmcloud.com/vulnerabilities/201673
https://www.citrix.com/downloads/workspace-app/windows/

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

Identifikátor

McAfee Total Protection - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť McAfee vydala bezpečnostnú aktualizáciu na svoj produkt McAfee Total Protection, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.05.2021

CVE

CVE-2021-23872, CVE-2021-23891

Zasiahnuté systémy

McAfee Total Protection (MTP) vo verzii staršej ako 16.0.32

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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.

Zdroje

https://service.mcafee.com/webcenter/portal/oracle/webcenter/page/scopedMD/s55728c97_466d_4ddb_952d_05484ea932c6/Page29.jspx;jsessionid=jGV4-2ALyxaTjAlZQuPTpviuoTtTkBImJrvrbbwjlIiM0rrR56Yf!525568826!-2001961837?wc.contextURL=%2Fspaces%2Fcp&articleId=TS103146&leftWidth=0%25&showFooter=false&showHeader=false&rightWidt=&_afrLoop=561893010122699#!%40%40%3FshowFooter%3Dfalse%26rightWidt%3D%26_afrLoop%3D561893010122699%26articleId%3DTS103146%26leftWidth%3D0%2525%26showHeader%3Dfalse%26wc.contextURL%3D%252Fspaces%252Fcp%26_adf.ctrl-state%3D95vna892k_4
https://exchange.xforce.ibmcloud.com/vulnerabilities/201691

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

Identifikátor

Omron CX-One CX-Server produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Omron vydala bezpečnostnú aktualizáciu na svoj produkt CX-One CX-Server, 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

11.05.2021

CVE

CVE-2021-27413

Zasiahnuté systémy

CX-One CX-Server vo verzii staršej ako 5.0.29.1

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-21-131-01

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

Identifikátor

Johnson Controls Sensormatic Tyco AI - bezpečnostná zraniteľnosť

Popis

Spoločnosť Johnson Controls vydala bezpečnostnú aktualizáciu svojho produktu Tyco AI, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje lokálnemu, autentifikovanému útočníkovi s používateľskými právomocami eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.05.2021

CVE

CVE-2021-3156

Zasiahnuté systémy

Johnson Controls Tyco AI verzie staršie 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.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-133-02

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

Identifikátor

Schneider Electric Modicon M241 a M251 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoje produkty Modicon M241 a M251 Logic Controllers.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej HTTP požiadavky, spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

11.05.2021

CVE

CVE-2021-22699

Zasiahnuté systémy

Modicon M241 Logic Controllers s firmware vo verzii staršej ako V5.1.9.14
Modicon M251 Logic Controllers s firmware vo verzii staršej ako V5.1.9.14

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN).

Zdroje

https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-130-05

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

Identifikátor

OPC UA Servers - viacero bezpečnostných zraniteľností

Popis

Spoločnosť OPC vydala bezpečnostnú aktualizáciu na svoj produkt UA Server, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

13.05.2021

CVE

CVE-2015-6096, CVE-2021-27432, CVE-2021-27434

Zasiahnuté systémy

OPC UA .NET Standard vo verzii staršej ako 1.4.365.48
OPC UA .NET Legacy (všetky verzie - ukončená podpora)

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN).

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-133-03
https://us-cert.cisa.gov/ics/advisories/icsa-21-133-04

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.9
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Mitsubishi Electric GOT a Tension Controller produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostné aktualizácie na produkty GOT a Tension Controller, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

11.05.2021

CVE

CVE-2021-20589

Zasiahnuté systémy

GOT2000 séria: GT27, GT25, GT23 modely vo verzii staršej ako 01.39.000
GOT2000 séria: GT21 model vo verzii staršej ako 01.40.000
GOT SIMPLE séria GS21 model vo verzii staršej ako 01.40.000
GT SoftGOT2000 vo verzii staršej ako 1.255R

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN).

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-131-02