2020ko Uztailaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Hainbat ahultasun Mitsubishi Electric etxearen produktu batzuetan

Argitalpen data: 2020/07/01

Garrantzia: Altua

Kaltetutako baliabideak:

Factory Automation ingeniaritzako software produktuen bertsioa batzuk kaltetu dira:

- CPU Module Logging Configuration Tool, 1.94Y bertsioa eta aurrekoak;
- CW Configurator, 1.010L bertsioa eta aurrekoak;
- EM Software Development Kit (EM Configurator), 1.010L bertsioa eta aurrekoak;
- GT Designer3?GOT2000), 1.221F bertsioa eta aurrekoak;
- GX LogViewer, 1.96A bertsioa eta aurrekoak;
- GX Works2, 1.586L bertsioa eta aurrekoak;
- GX Works3, 1.058L bertsioa eta aurrekoak;
- M_CommDTM-HART, 1.00A bertsioa;
- M_CommDTM-IO-Link, 1.02C bertsioa eta aurrekoak;
- MELFA-Works, 4.3 bertsioa eta aurrekoak;
- MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool, 1.004E bertsioa eta aurrekoak;
- MELSOFT FieldDeviceConfigurator, 1.03D bertsioa eta aurrekoak;
- MELSOFT iQ AppPortal, 1.11M bertsioa eta aurrekoak;
- MELSOFT Navigator, 2.58L bertsioa eta aurrekoak;
- MI Configurator, 1.003D bertsioa eta aurrekoak;
- Motion Control Setting, 1.005F bertsioa eta aurrekoak;
- MR Configurator2, 1.72A bertsioa eta aurrekoak;
- MT Works2, 1.156N bertsioa eta aurrekoak;
- RT ToolBox2, 3.72A bertsioa eta aurrekoak;
- RT ToolBox3, 1.50C bertsioa eta aurrekoak.

Azalpena:

Mitsubishi Electric PSIRT (Product Security Incident Response Team) enpresak CISA erakundeari 2 ahultasunen berri eman dio; bata larritasun handikoa eta bestea ertainekoa, XML (XXE) kanpo erakundearen erreferentziaren mugatze okerraren arloko eta baliabideen kontrolik gabeko kontsumoaren arlokoak. Factory Automation produktu batzuei eragiten diete.

Konponbidea:

Mitsubishi Electric enpresak gomendatu du kaltetutako erabiltzaileek software produktu bakoitzaren azken bertsioa deskargatzeko Mitsubishi Electricen deskarga zentrotik, eta eguneratzeko.

Xehetasuna:

- Ahultasunaren ondorioz, asmo txarreko erasotzaile batek artxibo bat bidal dezake, kaltetutako produktua exekutatzen duen ekipoan. Ahultasun horretarako, CVE-2020-5602 identifikatzailea esleitu da.
- Ahultasunaren ondorioz, asmo txarreko erasotzaile batek zerbitzuaren ukapen baldintza sor lezake (DoS) kaltetutako produktuan. Ahultasun horretarako, CVE-2020-5603 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura Kritikoak, Ahultasuna

Hainbat ahultasun Delta Electronics etxearen Delta Industrial Automation DOPSoft sisteman

Argitalpen data: 2020/07/01

Garrantzia: Handia

Kaltetutako baliabideak:

DOPSoft, 4.00.08.15 bertsioak eta aurrekoak.

Azalpena:

Argitaratutako 2 ahultasun horiek ondo baliatuz gero (larritasun handi eta ertainekoak), erasotzaile batek informazioa irakurri/aldatu, kode arbitrarioa exekutatu, edota aplikazioa blokeatu lezake.

Konponbidea:

4.00.08.17 bertsiora edo ostekoetara eguneratzea (2020ko uztailerako aurreikusita).

Xehetasuna:

- Mugetatik kanpoko hainbat irakurketa-ahultasunen ondorioz, urrutiko erasotzaile batek informazioa irakurri edota aplikazioa blokeatu lezake, bereziki diseinatutako proiektu-artxiboen prozesamenduaren bidez. Ahultasun horretarako, CVE-2020-10597 identifikatzailea esleitu da.
- Pilak gainezka egiteko bereziki diseinatutako proiektu-artxibo bat irekita, erasotzaile batek urrutiko kode exekuzioa baimendu lezake, informazioa zabaldu edo aldatu, edota aplikazioa blokearazi. Ahultasun horretarako, CVE-2020-14482 identifikatzailea esleitu da.

Etiketak: Eguneraketa, Azpiegitura Kritikoak, Ahultasuna

Nortek enpresaren Linear eMerge 50P/5000P sisteman hainbat ahultasun atzeman dira

Argitalpen data: 2020/07/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Linear eMerge 50P/5000P, 4.6.07 bertsioa (79330 berrikusketa) eta aurrekoak.

Azalpena:

Applied Risk enpresako Gjokok 5 ahultasunen berri eman dio CISA erakundeari; 3 larritasun kritikokoak dira, bat handikoa eta bestea ertainekoa. Horien bidez, urrutiko erasotzaile batek sistemaren erabateko kontrola lortu lezake.

Konponbidea:

v32-09a bertsiora eguneratzea.

Xehetasuna:

- Softwareak kanpo sarrerak erabiltzen ditu direktorio mugatu baten barruan egon beharko litzatekeen ibilbide bat eraikitzeko, baina ez ditu ondo neutralizatzen sekuentzia batzuk, "../", esaterako. Direktorio horretatik kanpoko kokapen batean konpondu litezke. Horren bidez, erasotzaile batek artxibo sistema zeharkatu lezake, mugatutako direktoriotik kanpo dauden artxibo edo direktorioetara heltzeko. Ahultasun horretarako, CVE-2019-7267 identifikatzailea esleitu da.
- Sarrerako datuetan karaktere bereziak neutralizatuta, erasotzaile batek komando arbitrarioak exekutatu litzake sistema eragilean. Ahultasun horretarako, CVE-2019-7269 identifikatzailea esleitu da.
- Firmwarearen eguneratzearen bidezko igoera-scriptaren bidez egitean artxiboen luzapena balioztatzen ez bada, gerta liteke baimenik gabeko urrutiko erasotzaile batek luzapen arbitrarioko artxiboak igotzea direktorio batera, aplikazioaren web erroaren barruan, eta web zerbitzariko pribilegioekin exekutatzea. Ahultasun horretarako, CVE-2019-7268 identifikatzailea esleitu da.
- Kaltetutako aplikazioa dela eta, ekintza zehatz batzuk egin litezke HTTP eskaeren bidez, eta eskaera horiek egiaztatu ahal izateko ez da konprobatzerik egiten. Horrela izanik, administrari pribilegioekin ekintzak burutu daitezke, konektatutako erabiltzaile batek webgune maltzur bat bisitatuz gero. Ahultasun horretarako, CVE-2019-7270 identifikatzailea esleitu da.
- Sarrera-datuak nahikoa ez egiaztatzearen ondorioz, urrutiko erasotzaile batek HTTP eskaera bat bidal dezake, bereziki diseinatua, egiaztatze-konprobatzea alde batera utzi eta aplikazioan baimenik gabe sartu ahal izateko. Ahultasun horretarako, CVE-2019-7266 identifikatzailea esleitu da.

Etiketak: Eguneraketa, Azpiegitura Kritikoak, Ahultasuna

Cross-site Scripting ahultasuna ABB System 800xA Information Manager sisteman

Argitalpen data: 2020/07/03

Garrantzia: Altua

Kaltetutako baliabideak:

System 800xA Information Manager, bertsioak:

- 5.1 Rev E/5.1 FP4 Rev E TC6 aurrekoak;
- 6.0.3.3, RU1 aurrekoak;
- 6.1, RU1 aurrekoak;

Azalpena:

William Knowles ikertzaileak ABB System 800xA Information Manager sisteman atzemandako Cross-site Scripting ahultasunaren berri eman du. Ahultasun horren bidez, zerbitzarian kode arbitrarioa injektatu eta exekutatu liteke.

Konponbidea:

Ahultasun hori ABB System 800xA Information Manager sistemaren honako bertsioetan zuzenduko da:

- 5.1 Rev E/5.1 FP4 E TC6: ABB enpresak 5.1 erabiltzaileei gomendatu die TC hau instalatzeko. Laguntza teknikoko zerbitzuan eska daiteke;
- 6.0.3.3 RU1: ABB enpresak 6.0.3 LTS erabiltzaileei gomendatu die 6.0.3.3 eguneratzeko eta RU1 instalatzeko;
- 6.1 RU1: ABB enpresak 6.1 erabiltzaileei gomendatu die bertsio honetara eguneratzeko.

6.0.3.3 eta 6.1 bertsioetarako Information Manager paketeak My ABB/My Control System ataletik deskarga daitezke.

Xehetasuna:

ABB System 800xA Information Manager sisteman atzemandako ahultasunaren ondorioz, erasotzaile batek kode arbitrarioa exekuta lezake Cross-site Scripting bidez. Ahultasun hori erabiltzeko, erasotzaileak Information Manager ahula instalatuta duen erabiltzaile bat engainatu behar du, horrek manipulatutako webgune bat bisitatzeko. Ahultasun horretarako CVE-2020-8477 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, SCADA, Ahultasuna.

Hainbat ahultasun OpenClinic GA sisteman

Argitalpen data: 2020/07/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- OpenClinic GA, 5.09.02 bertsioa;
- OpenClinic GA, 5.89.05b bertsioa;

Azalpena:

Brian D. Hysell ikertzaileak 12 ahultasunen berri eman zion CISA erakundeari. OpenClinic GA ospitale-informazioaren kudeaketa sistemari eragiten diote. 3 larritasun kritikokoak dira, 6 handikoak, eta 3 tartekoak.

Konponbidea:

OpenClinic GA erakundea ahultasun horien jakitun da, baina ez du konfirmaziorik eman. OpenClinic GA azken bertsiora eguneratzea gomendatu da, egungo zuzenketa guztiak bermatzeko.

Xehetasuna:

Larritasun kritikoko 3 ahultasunak ondoren deskribatu dira:

- Erasotzaile batek bezeroaren sarbide-kontrolak bertan behera utz litzake, edo saio bat funtzionaltasun mugatuz hasteko bereziki diseinatutako eskaera bat erabili. Horren ondorioz, administrari funtzioak exekutatu litezke, hala nola SQL kontsultak. Ahultasun horretarako, CVE-2020-14485 identifikatzailea erreserbatu da.
- Sistemak hirugarrenen software bertsioak ditu barne. Beren bizitza-zikloaren amaieran daude eta kodearen urrutiko exekuzioa baimendu lezaketen ahultasun ezagunak dituzte. Ahultasun horretarako, CVE-2020-14495 identifikatzailea erreserbatu da.
- Sistemak aurrez zehaztutako erabiltzaile-kontu bat dauka. Administrariren batek kontu hori desaktibatu ez badu soilik sar daiteke; horrela, erasotzaile batek saioa hasi eta komando arbitrarioak exekuta litzake (ez dio 5.89.05b bertsioari eragiten). Ahultasun horretarako, CVE-2020-14487 identifikatzailea erreserbatu da.

Gainerako ahultasunak erasotzaile batek baliatu litzake, honako ekintzaren bat burutzeko:

- Indarrezko erasoak, egiaztatze-saiakera gehiegiren aurrean mugatze desegokia izanagatik;
- Sisteman sartzea, egiaztatze-prozesu desegokiaren ondorioz;
- Informazio pribilegiatua lortzea, baimen faltagatik;
- Pribilegio handiegiekin komandoak exekutatzea;
- Kaltegarriak izan daitezkeen artxibo arbitrarioak kargatu eta exekutatzea, mugarik gabe;
- Artxibo konfidentzialak zabaldu edo kargatutako artxibo maltzurrak exekutatzea, kontrolatu gabeko ibilbide-sarbide baten ondorioz (path traversal);
- Baimendu gabeko komandoak exekutatzea;
- Nabigatzailean kode maltzurra exekutatzea, XSS baten bidez;
- Kredentzialak berreskuratzea, babes desegoki baten ondorioz.

Larritasun handi eta ertaineko ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2020-14484, CVE-2020-

14494, CVE-2020-14491, CVE-2020-14493, CVE-2020-14488, CVE-2020-14490, CVE-2020-14486, CVE-2020-14492 eta CVE-2020-14489.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Osasuna, Ahultasuna.

Hainbat ahultasun Grundfos Pumps Corporation erakundearen CIM 500 baliabidean

Argitalpen data: 2020/07/08

Garrantzia: Handia

Kaltetutako baliabideak:

CIM 500, 06.16.00 bertsioaren aurreko firmware bertsio guztiak.

Azalpena:

Marcin Dudek ikertzaileak, CERT.PL erakundekoa, bi ahultasunen berri eman zion CISA erakundeari, biak larritasun handikoak, funtzio kritikorako egiaztatze falta eta kredentzialen biltegiratze babesgabearen arlokoak.

Konpobidea:

Firmwarea 06.16.00 bertsiora eguneratzea eta eguneratzearen ostean kredentzialak aldatzea.

Xehetasuna:

- Kaltetutako produktuak pasahitzaren biltegiratze artxibo ez egiaztatuei erantzuten die. Ahultasun horretarako, CVE-2020-10605 identifikatzailea erreserbatu da.
- Kaltetutako produktuak formaturik gabeko kredentzialak biltegiratzen ditu. Horren ondorioz, informazio konfidentziala irakur daiteke, edo gailurako sarbidea duen baten batek sistemaren konfigurazioa alda lezake. Ahultasun horretarako, CVE-2020-10609 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Azpiegitura Kritikoak, Ahultasuna

Hainbat ahultasun Mitsubishi Electric enpresaren GOT2000 sisteman

Argitalpen data: 2020/07/08

Garrantzia: Kritikoa

Kaltetutako baliabideak:

GOT2000 CoreOS, -Y bertsioa eta aurrekoak, GT23, GT25 eta GT27 ereduak..

Azalpena:

Mitsubishi Electric erakundearen PSIRT taldeak CISA erakundeari eman zion ahultasun horien berri. Horiek baliatuta, urrutiko erasotzaile batek zerbitzuaren ukapena edo kodearen urrutiko kodea exekutatu litzake.

Konponbidea:

Mitsubishi enpresak erabiltzaileei gomendatu die honako urratsak jarraitzeko, CoreOS tresna azken bertsiora eguneratzeko:

- MELSOFT GT Designer3 (2000) baliabidea instalatzea, 1.240A bertsioa edo ostekoa, zure ordenagailu pertsonalean.
- MELSOFT GT Designer3 abiaraztea eta -Z bertsioko edo osteko bertsio bateko CoreOS SD txartelean kopiatzea.
- Ordenagailu pertsonaletik ateratako SD txartela kaltetutako baliabideetan sartzea eta CoreOS tresnaren azken bertsiora eguneratzea.

Xehetasuna:

Ahultasunak baliatuta, erasotzaile batek honako aukerak izan litzake:

- Gailua blokeatzea; horren ondorioz, kodearen urrutiko exekuzioa gerta liteke. Ahultasun horretarako, CVE-2020-5595 identifikatzailea esleitu da.
- TCP konexioaren zerbitzu ukapena eragitea. Ahultasun horretarako, CVE-2020-5596 identifikatzailea esleitu da.
- Zerbitzu ukapena eragin eta gailua blokeatzea. Ahultasun horretarako, CVE-2020-5597 identifikatzailea esleitu da.
- Baliabide sentikorrak eskuratzea, zerbitzu ukapena eragitea eta gailua blokeatzea. Ahultasun horretarako, CVE-2020-5598 identifikatzailea esleitu da.
- Zerbitzu ukapena eragitea. Ahultasun horretarako, CVE-2020-5599 identifikatzailea esleitu da.
- Informazio konfidentziala eskuratzea. Ahultasun horretarako, CVE-2020-5600 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitrua kritikoak, Ahultasuna

XML External Entity (XEE) ahultasuna Rockwell Automation erakundearen Studio 5000 Logix Designer tresnan

Argitalpen data: 2020/07/09

Garrantzia: Txikia

Kaltetutako baliabideak:

Logix Designer Studio 5000, 32.00, 32.01 eta 32.02 bertsioak.

Azalpena:

Pwn2Own lehiaketan zehar, Logix Designer Studio 5000 tresnan atzemandako ahultasun baten berri eman zen. Ahultasun hori baliatuta, erasotzaile batek artxibo maltzur bat parsetu lezake, eta, horren ondorioz, informazioa zabaldu.

Konponbidea:

AML edo RDF artxiboak erabiltzen dituzten Rockwell Automation erakundearen bezero guztiei gomendatzen zaie iturri ezezagunetako artxiborik ez onartzeko, eta kontuz ibiltzeko, ingeniaritza soziala ahultasun horretaz baliatu daiteke eta.

Xehetasuna:

Logix Designer Studio 5000 tresnaren 32.00, 32.01 eta 32.02 bertsioek hirugarrenen XML ikertzaile bat erabiltzen dute. AML eta RDF artxiboak onartzen ditu modu natiboan, kanpoko edozein erakundetatik. Arrakastaz erabilita, egiaztatu gabeko erasotzaile batek artxibo maltzur bat sortu lezake, eta, aztertuta, programaren bestelako baliabide edo host izenak zabaldu litzake. Ahultasun horretarako, CVE-2020-12025 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Ahultasuna

Hainbat ahultasun Softing Industrial Automation OPC sisteman

Argitalpen data: 2020/07/29

Garrantzia: Kritikoa

Kaltetutako baliabideak:

4.7.0 bertsioaren azken build delakoaren aurretiko OPC bertsio guztiak.

Azalpena:

Claroty erakundeko Uri Katz ikertzaileak bi ahultasunen berri eman dio CISAri, bata larritasun kritikokoa eta bestea handikoa. Motak: heap motako bufferraren gainezkatzea eta baliabideen kontrolik gabeko kontsumoa. Softing Industrial Automation etxearen OPC sistemari eragiten diote.

Konponbidea:

Softing Industrial Automation etxeak eguneratze bat argitaratu du, ahultasun horiek arintzeko. Bertsiorik eguneratuena, CISAren abisu horren unean, Softing Industrial Automation erakundearen webgunean aurki daiteke.

Xehetasuna:

- Kaltetutako produktuari heap motako buffer gainezkatzeak eragin ahal dio. Horrela, urrutiko erasotzaile batek kode arbitrarioa exekutatu lezake. Ahultasun horretarako, CVE-2020-14524 identifikatzailea erreserbatu da.
- Kaltetutako produktua baliabideen kontrolik gabeko kontsumoaren eraginpean dago, eta erasotzaile batek zerbitzu ukapena sortu lezake (DoS). Ahultasun horretarako, CVE-2020-14522 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun Secomea etxearen GateManager sisteman

Argitalpen data: 2020/07/29

Garrantzia: Kritikoa

Kaltetutako baliabideak:

GateManager, VPN zerbitzaria, 9.2c bertsioaren aurrekoak.

Azalpena:

Claroty erakundeko Sharon Brizinov eta Tal Keren ikertzaileek ahultasun batzuen berri eman diote CISAri. Horien bidez, erasotzaile batek balio negatibo bat bidal lezake eta datu arbitrarioak gainidatzi urrutitik, zerbitzu ukapena eragin, root komandoak eta bestelakoak exekutatu eta pasahitzak ikusi.

Konponbidea:

Azken bertsioetara eguneratzea. Secomea-ren webgunean daude eskuragarri.

Xehetasunak:

- Karaktere edo byte null delakoen neutralizazioaren ondorioz, erasotzaile batek balio negatibo bat bidal lezake, edo informazio arbitrarioa gainidatzi. Ahultasun horretarako, CVE-2020-14500 identifikatzailea erreserbatu da.
- Off-by-one errore baten ondorioz, urrutiko erasotzaile batek kode arbitrarioa exekuta lezake, edo zerbitzuaren ukapena eragin. Ahultasun horretarako, CVE-2020-14508 identifikatzailea erreserbatu da.
- Pasahitz barneratuak erabilita, erasotzaile batek root komandoak exekuta litzake, beste batzuen artean. Ahultasun horretarako, CVE-2020-14510 identifikatzailea erreserbatu da.
- Pasahitz ahulen hash erabilita, erasotzaile batek erabiltzailearen pasahitzak ikus litzake. Ahultasun horretarako, CVE-2020-14512 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Philips markaren DreamMapper sistemaren ahultasuna

Argitalpen data: 2020/07/31

Garrantzia: Ertaina

Kaltetutako baliabideak:

DreamMapper, 2.24 bertsioa eta aurrekoak.

Azalpena:

Informazio sentikorreko ahultasun bat argitaratu da. Erasotzaile batek errore mezuen mota desberdinen azalpen zehatza ikus lezake.

Konponbidea:

DreamMapper produktuaren eguneratze bat aurreikusi da 2021eko uztailerako.

Edozein zalantza baduzue, jarri harremanetan Philips-en laguntza zerbitzuarekin.

Xehetasunak:

Fitxategietan idatzitako informazioa erasotzaile batentzako erabilgarria izan daiteke, izan ere, errore mezu moten deskribapen zehatza ikus lezake. Ahultasun horretarako, CVE-2020-14518 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Osasuna, Ahultasuna.

Hainbat ahultasun Mitsubishi Electric etxearen produktu batzuetan

Argitalpen data: 2020/07/31

Garrantzia: Altua

Kaltetutako baliabideak:

- C Controller Interface Module Utility, bertsio guztiak;
- C Controller Module Setting eta Monitoring Tool, bertsio guztiak;
- CC-Link IE Control Network Data Collector, bertsio guztiak;
- CC-Link IE Field Network Data Collector, bertsio guztiak;
- CPU Module Logging Configuration Tool, 1.100E bertsioa eta aurrekoak;
- CW Configurator, 1.010L bertsioa eta aurrekoak;
- Data Transfer, bertsio guztiak;
- EZSocket, bertsio guztiak;
- FR Configurator SW3, bertsio guztiak;
- FR Configurator2, bertsio guztiak.
- GT Designer2 Classic, bertsio guztiak;
- GT Designer3 Version1 (GOT1000), bertsio guztiak;
- GT Designer3 Version1 (GOT2000), bertsio guztiak;
- GT SoftGOT1000 Version3, bertsio guztiak;
- GT SoftGOT2000 Version1, bertsio guztiak;
- GX Developer, 8.504A bertsioak eta aurrekoak,
- GX LogViewer, 1.100E bertsioa eta aurrekoak;
- GX Works2, bertsio guztiak;
- GX Works3, 1.063R bertsioa eta aurrekoak;

- Konfigurazio tresnak / C Controller modulurako monitorizazioa, bertsio guztiak;
- M_CommDTM-HART, 1.00A bertsioa;
- M_CommDTM-IO-Link, bertsio guztiak;
- MELFA-Works, bertsio guztiak;
- MELSEC WinCPU Setting Utility, bertsio guztiak;
- MELSEC iQ-R Series Motion Module, bertsio guztiak;
- MELSOFT iQ AppPortal, bertsio guztiak;
- MELSOFT EM Software Development Kit (EM Configurator), bertsio guztiak;
- MELSOFT FieldDeviceConfigurator, 1.03D bertsioa eta aurrekoak;
- MELSOFT Navigator, bertsio guztiak;
- MELSOFT Complete Clean Up Tool, bertsio guztiak;
- MH11 SettingTool Version2, 2.002C bertsioa eta aurrekoak;
- MI Configurator, bertsio guztiak;
- Motion Control Setting, 1.005F bertsioa eta aurrekoak;
- Motorizer, 1.005F bertsioa eta aurrekoak;
- MR Configurator2, bertsio guztiak;
- MT Works2, bertsio guztiak;
- MTConnect Data Collector, bertsio guztiak;
- MX Component, bertsio guztiak;
- MX MESInterface, bertsio guztiak;
- MX MESInterface-R, bertsio guztiak;
- MX Sheet, bertsio guztiak;
- Network Interface Board CC IE Control utility, bertsio guztiak;
- Network Interface Board CC IE Field Utility, bertsio guztiak;
- Network Interface Board CC-Link Ver.2 Utility, bertsio guztiak;
- Network Interface Board MNETH utility, bertsio guztiak;
- Position Board utility 2, bertsio guztiak;
- PX Developer, bertsio guztiak;
- RT ToolBox2, bertsio guztiak;
- RT ToolBox3, bertsio guztiak;
- SLMP Data Collector, bertsio guztiak.

Azalpena:

Applied Risk erakundeko ikerketa taldeak, eta Nozomi Networks-eko Younes Dragoni eta Claroty-ko Mashav Sapir ikertzaileek 3 ahultasunen berri eman diote CISAri, denak larritasun handikoak. Motak: baimen-arazoak, ibilbideetarako kontrolik gabeko sarbideak (path traversal) eta bilaketa ibilbidea edo komatxoen artean sartu gabeko elementua.

Konponbidea:

Kaltetutako produktuaren azken software bertsioa deskargatzea.

Xehetasuna:

- Ahultasun hori baliatuta, erasotzaile batek pribilegioetan gora egin lezake, edo programa maltzurrak exekutatu; horrela, zerbitzu ukapenaren baldintza sortu liteke (DoS), edo informazioa argitara eman, manipulatu edo suntsitu. Ahultasun horretarako, CVE-2020-14496 identifikatzailea erreserbatu da.
- Mitsubishi Electric Factory Automation etxearen hainbat produktuk ahultasun bat dute, eta, horren bidez, urrutiko erasotzaile batek kode arbitrarioa exekutatu lezake. Ahultasun horretarako, CVE-2020-14523 identifikatzailea erreserbatu da.
- Mitsubishi Electric Factory Automation etxearen software ingeniaritza produktu batzuek kode maltzurra exekutatzearen motako ahultasuna dute. Asmo txarreko erasotzaile batek ahultasun hori baliatu lezake informazioa lortu, aldatu edota zerbitzuaren ukapena sortzeko (Dos). Ahultasun horretarako, CVE-2020-14521 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Azpiegitura Kritikoak, Ahultasuna.

Hainbat ahultasun Yokogawa produktu batzuetan

Argitalpen data: 2020/07/31

Garrantzia: Altua

Kaltetutako baliabideak:

- CENTUM CS 3000 R3.08.10 - R3.09.50 (incluyendo CENTUM CS 3000 Entry Class);
- CENTUM VP R4.01.00 - R6.07.00 (incluyendo CENTUM VP Entry Class);
- B/M9000CS R5.04.01 - R5.05.01;
- B/M9000 VP R6.01.01 - R8.03.01.

Azalpena:

Positive Technologies erakundeko Nataliya Tlyapova eta Ivan Kurnakov ikertzaileek bi ahultasunen berri eman diote Yokogawa etxeari, biak larritasun handikoak, egiaztatze mota desegoki eta kontrolatu gabeko sarbideekin (path traversal).

Konponbidea:

- CENTUM CS 3000 R3.08.10 - R3.09.50: produktu honek ez dauka jarraipenik eta ez du ahultasunak konpontzeko partxerik edukiko; CENTUM VP azken bertsiora eguneratzea gomendatu da.
- CENTUM VP:
  - R4.01.00 - R4.03.00: produktuaren bertsio horiek ez daukate jarraipenik, eta ez dute ahultasunak konpontzeko partxerik edukiko; CENTUM VP azken bertsiora eguneratzea gomendatu da;
  - R5.01.00 - R5.04.20: eskuragarri dagoen azken bertsiora eguneratu (R5.04.20) eta partxea aplikatzea (R5.04.D1);
  - R6.01.00 - R6.07.00: eskuragarri dagoen azken bertsiora eguneratu (R6.07.00) eta partxea aplikatzea

(R6.07.11).

- B/M9000CS R5.04.01 - R5.05.01: produktu horri ez diote ahultasunek eragin, baina bai ekipo berean instalatutako CENTUM CS 3000 sistemak. CENTUM CS 3000 eguneratu behar bada, B/M9000CS ere eguneratu behar da, dagokion bertsiora.
- B/M9000 VP R6.01.01 - R8.03.01: produktu horri ez diote ahultasunek eragin, baina bai ekipo berean instalatutako CENTUM VP sistemak. CENTUM VP eguneratu behar bada, B/M9000 VP ere eguneratu behar da, dagokion bertsiora.

Xehetasunak:

- Ahultasun horren bidez, egiaztatu gabeko urrutiko erasotzaile batek bereziki diseinatutako komunikazio-paketeak bidal litzake. Ahultasun horretarako, CVE-2020-5608 identifikatzailea erreserbatu da.
- Ahultasun horren bidez, urrutiko erasotzaile batek edozein artxibo sortu edo gainean idatz dezake, edo edozein komando exekutatu. Ahultasun horretarako, CVE-2020-5609 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.