2021ko Apirilaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Múltiples vulnerabilidades en Rexroth ActiveMover de Bosch

Argitalpen data: 2021/04/05

Garrantzia: Handia

Kaltetutako baliabideak:

- Rexroth ActiveMover, honako konfigurazioekin: :
  - ?using Profinet communication module (Rexroth no. 3842 559 445)';
  - ?using EtherNet/IP communication module (Rexroth no. 3842 559 444)'. 3.0.26.x. bertsioaren aurrekoetarako

Azalpena:

Hainbat ahultasunen bidez, batzuk larritasun handikoak, komunikazio ziklikoa ustekabean galdu liteke, komunikazio aziklikoa eten, edo EtherNet/IP gailuaren blokeoa eragin, berreskuratzeko aukerarik gabe.

Konponbidea:

Bosch Rexroth sistemak produktua sare isolatu batean erabiltzea gomendatzen du, Interneterako sarbiderik gabe, eta honako arintze-neurriak aplikatzea:

- Sarean ahalik eta gutxien egotea erakusgai, eta Internet bidez sartu ezin dela ziurtatzea.
- Sare korporatiboko kaltetutako produktuak isolatzea, suebaki edo sare segmentazio bidez.
- Urruneko sarbidea beharrezkoa bada, erabili metodo seguruak, hala nola sare pribatu birtualak (VPN).

Xehetasuna:

- PROFINET IO Device V3 pila-protokoloak, V3.14.0.7 bertsioaren aurrekoa, ez ditu eskura dauden baliabideak behar bezala mugatzen Read Implicit Request zerbitzuak kudeatzean, eskaeraren edukiaren arabera. Horren ondorioz, komunikazio ziklikoa ustekabean galdu liteke, edota komunikazio aziklikoa eten. Ahultasun horretarako, CVE-2021-20986 identifikatzailea esleitu da.
- V2.13.0.21 bertsioaren aurreko Hilscher EtherNet/IP Core V2-ko memoria ustelkeria eta zerbitzu ukapenaren motako ahultasun baten bidez, erasotzaile batek kodea injektatu lezake sarearen bidez, edota gailuak berreskuratzeko aukerarik gabe blokeatzea eragin. Ahultasun horretarako, CVE-2021-20987 identifikatzailea esleitu da.

Etiketak: Komunikazioa, Azpiegitura kritikoak, Ahultasuna

Hainbat ahultasun Rockwell Automation erakundearen FactoryTalk sisteman

Argitalpen data: 2021/04/05

Garrantzia: Kritikoa

Kaltetutako baliabideak:

FactoryTalk AssetCentre, 10.00 bertsioa eta aurrekoak.

Azalpena:

Claroty erakundeko Sharon Brizinov eta Amir Preminger ikertzaileek larritasun kritikoko 9 ahultasunen berri eman diote Rockwell Automation erakundeari. Horien bidez, erasotzaile batek, urrunetik eta baimenik gabe, kode arbitrarioa exekuta lezake, edo SQL injekzioak burutu...

Konponbidea:

FactoryTalk AssetCentre 11 bertsiora edo osteko batera eguneratzea.

Arintze-neurri gehigarri moduan, fabrikatzaileak honakoa gomendatzen du:

- Segurtasun-funtzio integratuak erabiltzea, QA46277 gidari jarraituz.
- Softwarea administrari moduan ez exekutatzea.
- Microsoft AppLocker-en antzeko aplikazioak erabiltzea.
- Erabiltzaileentzako gutxieneko pribilegioen printzipioa jarraitzea.

Xehetasuna:

- AosService.rem, ArchiveService.rem eta LogService.rem zerbitzuetako datu ez fidagarrien deserializazio motako ahultasun baten bidez, urruneko eta baimenik gabeko erasotzaile batek komando arbitrarioak exekuta litzake. Larritasun horietarako CVE-2021-27462, CVE-2021-27466 eta CVE-2021-27470 identifikatzaileak esleitu dira, hurrenez hurren.
- IIS-ren urruneko komunikazio zerbitzuekin erlazionatutako funtzioen erabileraren mugetan ahultasunik izatekotan, erasotzaile batek, urrunetik eta baimenik gabe, isilpeko datuak alda litzake FactoryTalk AssetCentre delakoan. Ahultasun horretarako, CVE-2021-27474 identifikatzailea esleitu da.
- RACompare zerbitzuko SaveConfigFile funtzioaren ahultasun baten bidez, erasotzaile batek, urrunetik eta baimenik gabe, komando arbitrarioak exekuta litzake. Ahultasun horretarako, CVE-2021-27476 identifikatzailea esleitu da.
- SearchService, AosService.rem eta ArchiveService.rem zerbitzuen funtzioen ahultasunen bidez, erasotzaile batek, urrunetik eta baimenik gabe, SQL arbitrarioak exekuta litzake. Larritasun horietarako CVE-2021-27472, CVE-2021-27468 eta CVE-2021-27464 identifikatzaileak esleitu dira, hurrenez hurren.
- FactoryTalk AssetCentre osagaien urruneko NET endpoint-etako datu ez fidagarrien deserializazio arloko ahultasun baten bidez, erasotzaile batek, urrunetik eta baimenik gabe, zerbitzari nagusirako eta erlazionatutako makinetarako sarbidea izan lezake. Ahultasun horretarako, CVE-2021-27460 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Zerbitzu ukapena hainbat Hitachi ABB Power Grids produktutan

Argitalpen data: 2021/04/07

Garrantzia: Handia

Kaltetutako baliabideak:

- Relion 670 series, honako bertsioen errebisio guztiak: 1.1, 1.2.3, 2.0, 2.2.2 eta 2.2.3;
- Relion 670 series, 1.1, 1.2, eta 1.3 bertsioen errebisio guztiak;
- Relion 670/650 series, 2.1 eta 2.2.0 bertsioen errebisio guztiak;
- Relion 670/650/SAM600-IO series 2.2.1 bertsioa, bertsio guztiak;
- RTU500 CMU, 7.x, 8.x, 9.x, 10.x, 11.x eta 12.x firmware bertsioak;
- REB500, 7.3, 7.4, 7.5 7.6, 8.2 eta 8.3 bertsioak;
- TEGO1 zerbitzu unitatea FOX615, ESW-rekin, R1D02 bertsioa eta aurrekoak;
- MSM, 2.1.0 bertsioaren aurreko guztiak;
- GMS600, 1.3.0 bertsioa eta aurrekoak;
- PWC600, 1.0 eta 1.1 bertsioak.

Azalpena:

Markus Mahrla, GAI NetConsult GmbH erakundeko ikertzaileak, eta Lars Lengersdorf, Amprion GmbH erakundekoak, larritasun handiko ahultasun baten berri eman diote Hitachi ABB Power Grids enpresari. Horren bidez, kaltetutako gailua berrabiarazi liteke, eta zerbitzu-ukapena eragin (DoS).

Konponbidea:

Hitachi ABB Power Grids erakundeak erabiltzaileei gomendatu die eguneratzeak ahalik eta azkarren aplikatzeko, ahultasuna konpontzen duen *firmware* bertsio zehatza lortzeko fabrikatzailearekin kontaktuan jarriz.

Erreferentziazko loturaren *4.MITIGATIONS* atalean fabrikatzaileak ahultasun hori arintzeko garatutako bertsio berriak kontsulta litezke, bai argitaratutakoak, baita planeatutakoak ere.

Xehetasuna:

IEC sarerako sarbidea duen, IEC 61850 sarbide-puntuen IP helbideak ezagutzen dituen eta eraso bat erreproduzitzen dakien erasotzaile batek gailua berrabiaraztea eragin lezake. Horrela, minutu batez edo lan egiteko aukerarik gabe utziko luke. Ahultasun horrek IEC 61850 interfazeak dituzten produktuei soilik eragiten die. CVE-2021-27196 identifikatzailea esleitu da ahultasun horretarako.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Osoen azpigainezkatzea FATEK Automation

erakundearen WinProladder sisteman

Argitalpen data: 2021/04/09

Garrantzia: Altua

Kaltetutako baliabideak:

WinProladder, 3.30 bertsioa eta aurrekoak.

Azalpena:

Francis Provencher ikertzaileak, Trend Microren ZDIrekin elkarlanean, larritasun handiko ahultasun baten berri eman dio CISAri. Horren bidez, erasotzaile batek kode arbitrarioa exekuta lezake.

Konponbidea:

Momentuz, FATEK Automation erakundeak ez du konponbiderik argitaratu. Informazio gehiago behar baduzu, jarri harremanetan fabrikatzailearekin.

Xehetasunak:

Osoen azpigainezkatze motako ahultasun baten bidez, mugetatik kanpoko idazketa gerta liteke, eta, erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun horretarako, CVE-2021-2748 identifikatzailea esleitu da.

Etiketak: Azpiegitura kritikoak, Ahultasuna

Siemens segurtasun oharrak, 2021eko apirila

Argitalpen data: 2021/04/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Tecnomatix RobotExpert, 16.1 bertsioaren aurreko guztiak;
- Nucleus NET, bertsio guztiak;
- Nucleus RTOS, kaltetutako DNS moduluak barne hartzen dituzten bertsioak;
- Nucleus Source Code, kaltetutako DNS moduluak eta IPv6 stack barne hartzen duten bertsio guztiak;
- Nucleus ReadyStart, bertsio guztiak;
- Nucleus 4, 4.1.0 bertsioaren aurreko guztiak;
- VSTAR, kaltetutako DNS moduluak eta IPv6 stack barne hartzen dituzten bertsioak;
- SCALANCE X200-4P IRT, 5.5.1aren aurreko bertsio guztiak;
- SCALANCE X201-3P IRT, 5.5.1aren aurreko bertsio guztiak;
- SCALANCE X201-3P IRT PRO, 5.5.1aren aurreko bertsio guztiak;
- SCALANCE X202-2 IRT, 5.5.1aren aurreko bertsio guztiak;
- SCALANCE X202-2P IRT (SIPLUS NET aldaerak barne), 5.5.1aren aurreko bertsio guztiak;
- SCALANCE X202-2P IRT PRO, 5.5.1aren aurreko bertsio guztiak;
- SCALANCE X204 IRT, 5.5.1aren aurreko bertsio guztiak;
- SCALANCE X204 IRT PRO, 5.5.1aren aurreko bertsio guztiak;
- SCALANCE X204-2 (SIPLUS NET aldaerak barne), bertsio guztiak;
- SCALANCE X204-2FM, bertsio guztiak;
- SINEMA Remote Connect Server, 3.0ren aurreko bertsio guztiak;
- TIM 4R-IE (SIPLUS NET aldaerak barne), bertsio guztiak;
- TIM 4R-IE DNP3 (SIPLUS NET aldaerak barne), bertsio guztiak;
- Solid Edge SE2020, SE2020MP13 bertsioaren aurreko guztiak;
- Solid Edge SE2020, SE2020MP13 bertsioa (CVE-2020-26997, CVE-2021-25678 eta CVE-2021-27382 ahultasunek soilik eragiten diote);
- Solid Edge SE2021, SE2021MP4 bertsioaren aurreko guztiak;
- SIMOTICS CONNECT 400:
  - 0.5.0.0ren aurreko bertsio guztiak;
  - 0.5.0.0 bertsio guztiak eta ostekoak CVE-2021-25677 ahultasunaren mende baino ez daude.
- Control Center Server (CCS):
  - 1.5.0en aurreko bertsio guztiak;
  - 1.5.0 bertsio guztiak eta ostekoak CVE-2019-18340 ahultasunaren mende baino ez daude.
- Siveillance Video Open Network Bridge, honako bertsioak:
  - 2020 R3,
  - 2020 R2,
  - 2020 R1,
  - 2019 R3,
  - 2019 R2,
  - 2019 R1,
  - 2018 R3,
  - 2018 R2.
- LOGO! Soft Comfort, bertsio guztiak.

Azalpena:

Siemensek produktu batzuen inguruan hainbat segurtasun-eguneratze argitaratu ditu, bere hileroko jakinarazpenean.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneratzeak Siemens deskarga paneletik deskargatu daitezke. Eguneratzerik gabeko produktuetarako, Erreferentzien atalean azaldutako arintze-neurriak aplikatu behar dira.

Xehetasunak:

Siemensek, segurtasun partxeei buruzko hileroko jakinarazpenean, 31 segurtasun-abisu eman ditu; horietatik 17 eguneratzeak dira.

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Mugetatik kanpoko idazketa,
- Zerbitzua ukatzea,
- Bufferrak gainezka egitea,
- DNS cachea pozoitzea,
- DNS spoofing,
- Bukle infinitua,
- Memoria-ihesa,
- Egiaztatzerik eza,
- man-in-the-middle,
- Egiaztatze ez nahikoa,
- Sarrerako balioztatze okerra,
- Informazio sentikorra zabaltzea,
- Karrera baldintza,
- Kodearen exekuzioa;
- Mugetatik kanpoko irakurketa,
- Behar besteko ausazkotasunik gabeko balioen erabilera,
- Kredentzialak testu argi gisa erabiltzea,
- Ibilbide edo direktorio mugatu baterako ibilbidearen mugatze desegokia (path traversal),
- DLL hijacking,
- Algoritmo kriptografiko ez seguruaren erabilera,
- SQL injekzioa,
- XSS,
- Logging kudeaketa ez nahikoa.

Ahultasun horietarako, honako identifikatzaileak erreserbatu dira: CVE-2021-25670, CVE-2020-15795, CVE-2020-27009, CVE-2021-25668, CVE-2021-25669, CVE-2021-27393, CVE-2021-25663, CVE-2021-25664, CVE-2019-19956, CVE-2020-7595, CVE-2015-5219, CVE-2015-7855, CVE-2015-7871, CVE-2015-7973, CVE-2015-7974, CVE-2015-7977, CVE-2015-7979, CVE-2015-7705, CVE-2015-8138, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, CVE-2016-4953, CVE-2016-4954, CVE-2020-28385, CVE-2020-26997, CVE-2021-25678, CVE-2021-27380, CVE-2021-27382, CVE-2020-27736, CVE-2020-27737, CVE-2020-27738, CVE-2021-25677, CVE-2020-27736, CVE-2020-27737, CVE-2020-27738, CVE-2021-25677, CVE-2021-27392, CVE-2020-25243, CVE-2020-25244, CVE-2019-13947, CVE-2019-18337, CVE-2019-18338, CVE-2019-18340, CVE-2019-18341, CVE-2019-18342, CVE-2019-19290, CVE-2019-19291, CVE-2019-19292, CVE-2019-19293, CVE-2019-19294 eta CVE-2019-19295.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, Pribatutasuna, Siemens, Ahultasuna.

Schneider Electric erakundearen produktuen ahultasunak

Argitalpen data: 2021/04/14

Garrantzia: Altua

Kaltetutako baliabideak:

- SHFK-MT-104 DIVG.424327.104-14;
- SHFK-MT-104 DIVG.424327.104-09;
- SHFK-MT-104 DIVG.424327.104-08;
- SHFK-MT-104 DIVG.424327.104-24;
- SHFK-MT-104 DIVG.424327.104-10;
- SHFK-MT-104 DIVG.424327.104-27;
- SHFK-MT-104 DIVG.424327.104-28;
- SHFK-MT-104 DIVG.424327.104-30;
- SHFK-MT-104 DIVG.424327.104-25;
- SHASU-MT-107 DIVG.424327.107-02;
- SHASU-MT-107 DIVG.424327.107-01;
- SHAIIS-MT-111 DIVG.424327.111-04;
- SHAIIS-MT-111 DIVG.424327.111-06;
- SHAIIS-MT-111 DIVG.424327.111-08;
- SHAIIS-MT-111 DIVG.424327.111-11;
- SHAIIS-MT-111 DIVG.424327.111-02;
- SHAIIS-MT-111 DIVG.424327.111-14;
- SHAIIS-MT-111 DIVG.424327.111-16;
- SHAIIS-MT-111 DIVG.424327.111-19;
- SHAIIS-MT-111 DIVG.424327.111-20;
- SHAIIS-MT-111 DIVG.424327.111-12;
- C-Bus Toolkit, 1.15.7 bertsioa eta aurrekoak.

Azalpena:

Hainbat ahultasun argitaratu dira, 5 larritasun handikoak eta 2 tarteko larritasunekoak. Horien bidez, erasotzaile batek NTLM MIC konprobazioa saihestu lezake, edota pribilegioetan gora egin.

Konponbidea:

Honakoak aplikatzea:

- CVE-2019-1040rako Microsoft partxea
- CVE-2019-0803rako Microsoft partxea;
- C-Bus Toolkit 1.15.8 bertsiora eguneratzea.

Xehetasunak:

- Win32k osagaiaren ahultasun batek, memorian objektuen kudeaketa desegokia egitearen motakoa, erasotzaile bati pribilegioetan gora egiteko aukera eman liezaioke. Ahultasun horretarako, CVE-2019-0803 identifikatzailea esleitu da.
- Pribilegioen kudeaketa desegokiaren motako ahultasun baten ondorioz, urruneko kodea exekutatu liteke, pribilegiorik gabeko erabiltzaile batek artxibo bat aldatzen duenean. Ahultasun horretarako, CVE-2021-22716 identifikatzailea esleitu da.
- Direktorio mugatu baterako ibilbide baten izenaren mugatze desegokiaren ondorioz (path traversal), kodearen urruneko exekuzioa burutu liteke, konfigurazio artxiboak prozesatzean. Ahultasun horretarako, CVE-2021-22717 identifikatzailea esleitu da.
- Direktorio mugatu baterako ibilbide baten izenaren mugatze desegokiaren ondorioz (path traversal), kodearen urruneko exekuzioa burutu liteke, konfigurazio artxiboak zaharberritzean. Ahultasun horretarako, CVE-2021-22718 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2021-22720 eta CVE-2019-1040.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Schneider Electric, Ahultasuna, Windows.

Baliabideen liberazio okerra JTEKT Corporation erakundearen TOYOPUC produktuetan

Argitalpen data: 2021/04/14

Garrantzia: Altua

Kaltetutako baliabideak:

- Honako TOYOPUC-PC10 produktuen bertsio guztiak. Serieak:
  - PC10G-CPU TCC-6353,
  - PC10GE TCC-6464,
  - PC10P TCC-6372,
  - PC10P-DP TCC-6726,
  - PC10P-DP-IO TCC-6752,
  - PC10B-P TCC-6373,
  - PC10B TCC-1021,
  - PC10B-E/C TCU-6521,
  - PC10E TCC-4737.
- Honako TOYOPUC-Plus produktuen bertsio guztiak. Serieak:
  - Plus CPU TCC-6740,
  - Plus EX TCU-6741,
  - Plus EX2 TCU-6858,
  - Plus EFR TCU-6743,
  - Plus EFR2 TCU-6859,
  - Plus 2P-EFR TCU-6929,
  - Plus BUS-EX TCU-6900.
- Honako TOYOPUC-PC3J/PC2J produktuen bertsio guztiak. Serieak:
  - FL/ET-T-V2H THU-6289,
  - 2PORT-EFR THU-6404.

Azalpena:

Younes Dragoni, Nozomi Networks erakundeko ikertzaileak, larritasun handiko ahultasun baten berri eman dio CISAri. Horren bidez, erasotzaile batek gailuen arteko Ethernet komunikazioak eten litzake.

Konponbidea:

JTEKT Corporation erakundeak erabiltzaileei gomendatu die CISAren abisuaren 4. MITIGATIONS atalean azaldutako urratsak jarraitzeko.

Informazio gehiago jasotzeko eskaerak JTEKT Corporation erakundera bidal litezke: .

Xehetasunak:

Kaltetutako produktuaren Ethernet komunikazioa open state moduan uzten badu erasotzaile batek, Ethernet komunikazioak ezin dira beste gailu batzuekin ezarri, lotura-parametroen konfigurazioaren arabera. Ahultasun horretarako, CVE-2021-27458 identifikatzailea esleitu da.

Etiketak: Komunikazioa, Azpiegitura kritikoak, Ahultasuna

Baimenen esleipen desegokia baliabide

kritikoetarako, Advantech erakundearen WebAccess/SCADA sisteman

Argitalpen data: 2021/04/14

Garrantzia: Altua

Kaltetutako baliabideak:

WebAccess/SCADA, 9.0.1 bertsioa eta aurrekoak.

Azalpena:

Trend Microren TXOne IoT/ICS Security Research Labs taldeko Chizuru Toyama ikertzaileak larritasun handiko ahultasun baten berri eman dio CISAri. Horren bidez, urruneko erasotzaile batek pribilegioetan gora egin lezake.

Konponbidea:

9.0.3 bertsiora edo osteko batera eguneratzea.

Xehetasunak:

WebAccess/SCADA atarian baliabide kritikoetarako baimenen esleipen desegokiaren motako ahultasun bat egotearen ondorioz, urruneko erasotzaile batek, pribilegio gutxirekin, administrari pasahitza eguneratu lezake eta saioa horrela asi, sisteman pribilegioetan gora egieko. Ahultasun horretarako, CVE-2021-22669 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, IoT, SCADA, Ahultasuna.

Hainbat ahultasun OpenClinic GA sistemaren webgunean

Argitalpen data: 2021/04/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

OpenClinic GA, 5.173.3 bertsioa;

Azalpena:

Yuri Kramarz, Cisco Talos erakundeko ikertzaileak hainbat ahultasun antzeman ditu: SQL injekzio motakoak, komando injekzio motakoak edota pribilegioetan gora egitearen motakoak. Horiek guztiek OpenClinic GA sistemaren webguneari eragiten diote. Bat larritasun kritikokoa da, beste bat larritasun handikoa, eta gainerakoak tarteko larritasunekoak.

Konponbidea:

OpenClinic GA 5.173.3 bertsioaren osteko batera eguneratzea.

Xehetasunak:

- Bereziki diseinatutako web eskaeren bidez, zerbitzarian komandoak exekuta litezke, komandoen injekzio motako ahultasun baten ondorioz. Erasotzaile batek, baimenik gabe, datu-basearen exfiltrazio bat egiteko aukera baliatu lezake, erabiltzailearen kredentzialak eskuratuz, eta azpiko sistema eragilea konprometitu. Ahultasun kritiko horretarako, CVE-2020-27227 identifikatzailea esleitu da.
- Bitarra gainidaztearen ondorioz, pribilegioetan gora egin liteke, instalazio-funtzionalitatean berez desegokiak diren baimenen ahultasun bat egonez gero. Erasotzaile batek artxibo bat ordeztu lezake ahultasun hori baliatzeko. Ahultasun kritiko horretarako, CVE-2020-27228 identifikatzailea esleitu da.

Tarteko larritasuneko gainerako ahultasunetarako, honako identifikatzaileak esleitu dira: CVE-2020-27226, CVE-2020-27229, CVE-2020-27230, CVE-2020-27231, CVE-2020-27232, CVE-2020-27233, CVE-2020-27234, CVE-2020-27235, CVE-2020-27236, CVE-2020-27237, CVE-2020-27238, CVE-2020-27239, CVE-2020-27240, CVE-2020-27241, CVE-2020-27242, CVE-2020-27243, CVE-2020-27244, CVE-2020-27245 eta CVE-2020-27246.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Osasuna, Ahultasuna.

Hainbat ahultasun Eaton produktu batzuetan

Argitalpen data: 2021/04/14

Garrantzia: Altua

Kaltetutako baliabideak:

- Eaton Intelligent power Manager (IPM), 1.69 bertsioaren aurreko guztiak;
- Eaton Intelligent Power Manager Virtual Applicance (IPM VA), 1.69 bertsioaren aurreko guztiak;
- Eaton Intelligent Power Protector (IPP), 1.68 bertsioaren aurreko guztiak.

Azalpena:

Claroty research erakundeko Amir Preminger ikertzaileak larritasun handiko 6 ahultasunen berri eman du. Horien bidez, erasotzaile batek erabiltzaileak gehitu litzake datu-basean, komando arbitrarioak exekutatu, informazioa ezabatu eta kode maltzurra kargatu.

Konponbidea:

Eaton IPM 1.69 bertsiora eguneratzea, eta Eaton IPP 1.68 bertsiora eguneratzea.

Xehetasunak:

- IPMko SQL injekzio arloko ahultasun baten bidez, baimena lortu duen erasotzaile batek erabiltzaileak gehitu litzake datu-basean, bereziki diseinatutako pakete bat bidaliz. Ahultasun horretarako, CVE-2021-23276 identifikatzailea esleitu da.
- IPMko ebaluazio injekzioaren motako ahultasun baten ondorioz, softwareak ez du erabiltzailearen kodearen sintaxia neutralizatzen loadUserFile funtzioa deitu aurretik, beraz, baimenik gabeko erasotzaile batek funtziorako sarbidea kontrola lezake, eta komando arbitrarioak exekutatu. Ahultasun horretarako, CVE-2021-23277 identifikatzailea esleitu da.
- server/maps_srv.js eta meta_driver_srv.js eremuetako sarbide-balioztatze oker baten ondorioz, erasotzaile batek, baimenarekin ala gabe, IPM softwarea instalatuta dagoen sistemako artxiboak ezabatu litzake, bereziki diseinatutako paketeak bidaliz. Ahultasun horietarako CVE-2021-23278 eta CVE-2021-23279 identifikatzaileak erreserbatu dira.
- IPM eremuan artxiboen karga arbitrarioaren arloko ahultasun bat egotearen ondorioz, erasotzaile batek, baimenarekin, NodeJS artxibo maltzur bat kargatu lezake, edota komando arbitrarioak exekutatu, bereziki diseinatutako pakete bat bidaliz. Ahultasun horretarako, CVE-2021-23280 identifikatzailea esleitu da.
- IPM eremuan kode-injekzioaren motako ahultasun bat egotearen ondorioz, erasotzaile batek, baimenik gabe, bereziki diseinatutako pakete bat bidal lezake, IPM SNMP zerbitzari batera konektatzeko eta kode arbitrarioa exekutatzeko. Ahultasun horretarako, CVE 23281 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna

Hainbat ahultasun EIPStackGroup erakundearen OpENer EtherNet/IP sisteman

Argitalpen data: 2021/04/16

Garrantzia: Handia

Kaltetutako baliabideak:

OpENer EtherNet/IP, commits eta 2021/02/10aren aurreko bertsioak.

Azalpena:

Tal Keren eta Sharon Brizinov, Claroty erakundeko ikertzaileek, larritasun handiko 4 ahultasunen berri eman diote CISAri. EIPStackGroup erakundearen OpENer EtherNet/IP sistemari eragiten diote eta zerbitzuaren ukapen baldintza bat eta informazioa erakusgai geratzea ekarri lezakete (DoS).

Konponbidea:

OpENer mantentzaileak eskuragarri dauden azken commits delakoak aplikatzea gomendatzen du.

Xehetasuna:

- Erasotzaile batek kaltetutako gailuetara bidalitako bereziki diseinatutako pakete batek zerbitzuaren ukapena eragin lezake (DoS). Ahultasun horietarako CVE-2021-27478, CVE-2021-27500 eta CVE-2021-27498 identifikatzaileak esleitu dira.
- Erasotzaile batek bidalitako bereziki diseinatutako pakete batek datu arbitrarioak irakurtzeko aukera eman lezake. Ahultasun horretarako, CVE-2021-27482 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun LANTIME firmwarea duten Meinberg produktuetan

Argitalpen data: 2021/04/21

Garrantzia: Handia

Kaltetutako baliabideak:

LANTIME firmwarea duten produktu guztiak, V7.02.003 eta V6.24.028 bertsioen aurrekoak.

Firmware hori LANTIME markako M serie, IMS serie eta SyncFire produktuetan erabiltzen da.

Azalpena:

Meinberg fabrikatzaileak LANTIME *firmwarearen* bertsio berrien berri eman du. Hirugarrenen osagai integratuetako hainbat ahultasun zuzentzen dituzte, hain zuzen ere, OpenSSL, sudo eta LTOS-Web-Interface web interfazeari eragiten dioten

ahultasunak dira. Horien bidez, erasotzaile batek komunikazioen zifratua aldatu lezake, pribilegioetan gora egin, komandoak injektatu edota Cross-Site-Scripting motako ahultasun bat exekutatu.

Konponbidea:

LANTIME firmwarea V7.02.003 eta V6.24.028 bertsioetara eguneratzea gomendatzen da. Fabrikatzailearen webgunean daude eskuragarri.

Xehetasuna:

LANTIME firmwarean konpondutako eta hirugarrenen osagai integratuei eragiten dieten ahultasunak honakoak dira:

- OpenSSL: CVE-2021-3450, CVE-2021-23840, CVE-2021-23841 eta CVE-2021-23840;
- sudo: CVE-2021-3156.

Meinberg fabrikatzaileak bere web interfazeari eragiten dioten ahultasunak ere konpondu ditu. Horien bidez, erasotzaile batek komandoen injekzio edota Cross-Site-Scripting motako erasoak burutu litzake. Antza denez, SyncMon web interfazearen eremu batzuetarako balioztatze-faltaren ondorioz gertatzen dira. Ahultasun horietarako ez da CVE identifikatzailerik erreserbatu.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, SCADA, SSL/TLS, Ahultasuna.

Hainbat ahultasun Delta Electronics-en produktuetan

Argitalpen data: 2021/04/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- COMMGR, 1.12 bertsioa eta aurrekoak;
- CNCSoft. 1.01.28 bertsioa (ScreenEditor 1.01.2 bertsioa) eta aurrekoak;
- CNCSoft-B, 1.0.0.3 bertsioa eta aurrekoak.

Azalpena:

Peter Cheng ikertzaileak, Elex CyberSecurity, Inc. Erakundeko CyberSpace Non-Attack Research Institute zentrokoa, eta Natnael Samson ikertzaileak, Trend Micro-ren ZDIrekin elkarlanean, 4 ahultasunen berri eman diote CISAri: bat larritasun kritikokoa eta 3 larritasun handikoak. Horien bidez, erasotzaile batek kodearen urrutiko exekuzioa burutu lezake (RCE), kaltetutako aplikazioaren akatsa eragin, edota kode arbitrarioaren exekuzioa eragin.

Konponbidea:

Honako bertsioetara eguneratzea:

- COMMGR 1.13;
- CNCSoft ScreenEditor 1.01.30;
- CNCSoft-B 1.0.0.4 edo ostekoak.

Xehetasuna:

- Kaltetutako produktua pilan oinarritutako bufferraren gainezkatze (stack) baten arriskupean dago. Horren bidez, erasotzaile batek urruneko kodea exekuta lezake, eta horrek zerbitzuaren ukapena eragin lezake (DoS) aplikazioen zerbitzarian. Ahultasun kritiko horretarako, CVE-2021-27480 identifikatzailea esleitu da.
- Produktua mugetatik kanpoko irakurketaren arriskupean dago, eta, horren eraginez, erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun handi horietarako CVE-2021-22668 eta CVE-2021-22660 identifikatzaileak erreserbatu dira.
- Kaltetutako produktua mugetatik kanpoko idazketaren arriskupean egon daiteke; horren ondorioz, erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun handi horretarako CVE-2021-22664 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, Osasuna, Ahultasuna

---

Hainbat ahultasun Rockwell Automation erakundearen Stratix kommutadoreetan

Argitalpen data: 2021/04/21

Garrantzia: Handia

Kaltetutako baliabideak:

- Stratix 5800: 16.12.01 bertsioak eta aurrekoak;
- Stratix 8000: 15.2 (7) E3 bertsioak eta aurrekoak;
- Stratix 5700: 15.2 (7) E3 bertsioak eta aurrekoak;
- Stratix 5410: 15.2 (7) E3 bertsioak eta aurrekoak;
- Stratix 5400: 15.2 (7) E3 bertsioak eta aurrekoak.

Azalpena:

Ciscoko ikertzaile batzuek Rockwell Automation erakundeari jakinarazi diote Stratixek kudeatutako kommutadore industrialetan ahultasunak daudela. Horien bidez, erasotzaile batek hainbat ahultasun mota eragin litzake: zerbitzu ukapena, baimenik gabe pribilegioetan gora egitea, web saioak bahitzea, ibilbide erlatiboetarako sarbide ez baimenduak, edota komandoen injekzioa produktu kaltetuetan.

Konponbidea:

Rockwell Automationek honako konponbideak aplikatzea gomendatzen du:

- Stratix 5800: 17.04.01 bertsioa edo ostekoa instalatzea, eta, posible bada, DECnet protokoloa guztiz edo interfazeka desaktibatzea.
- Stratix 8300: produktua konponbide eguneratuago batera migratzea.

Kaltetutako produktu guztietarako gomendioak: gutxieneko pribilegioen erabiltzailearen printzipioa aplikatzea, eta erabiltzailearen kontuetarako sarbidea soilik beharrezko langileei ematea. Fabrikatzailearen oharra kontsulta daiteke, informazio gehiago izateko.

Rockwell Automation erakundea partxe berriak egiteko lanean ari da, ahultasun horiek konpontzeko. Bitartean, arintze-neurri moduan, honako gomendioak eman ditu:

- Kontrol industrialeko sistemak dauden sareetan erabiltzea, sareko azpiegitura segmentatzea firewall bidez, baimenik gabeko iturrien trafikoa saihesteko, edo enpresaren sarean.
- Aukera ematen duten produktuetan, etengailu baten konfigurazioa erabiltzea hardware moduan, baimendu gabeko aldaketak eta abar blokeatzeko.
- Gailuetara ekipo fidagarrietatik konektatzea, aplikatutako oinarrizko neurriekin, hala nola antibirus edo antimalware programak erabiltzea, edo ekipo eguneratuak, Interneterako sarbide mugatuarekin.
- Kontrol gailu edota azpisistema guztietarako sarean ahalik eta gutxien egotea, eta Internet bidez sartu ezin dela ziurtatzea.
- Urrutiko sarbidea behar denean, erabili metodo seguruak, hala nola sare pribatu birtualak (VPN).

Xehetasuna:

Ciscok hainbat ahultasunen berri eman dio Rockwell Automation erakundeari. Horien bidez, CLI edo uPNP bidez eta Cisco IOS eta Cisco IOS XE software produktuen bidez, Stratix kommutadoreak kaltetu litezke. Ahultasun horietako batzuen bidez, baimena lortzen duen erasotzaile batek protokolo industrial arrunteko pasahitza berreskura lezake (CIP), eta gero urrunetik kaltetutako gailua konfiguratu, erabiltzaile moduan, edo DECnet protokoloaren bidez zerbitzu ukapena eragin.

Gainera, ahultasun bat antzeman da Stratix 5800 kommutadoreetan. Horren bidez, baimenik gabeko erasotzaile fisiko batek kode iraunkorra exekuta lezake arrankatzeko unean.

Ahultasun honi honako identifikatzaileak esleitu zaizkio: CVE-2021-1392, CVE-2021-1403, CVE-2021-1352, CVE-2021-1442, CVE-2021-1452, CVE-2021-1443, CVE-2021-1220 eta CVE-2021-1356.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, SCADA, Ahultasuna.

XSS ahultasuna Hitachi ABB Power Grids etxearen Ellipse APM produktuetan

Argitalpen data: 2021/04/21

Garrantzia: Tartekoa

Kaltetutako baliabideak:

- Ellipse APM, 5.3.0.1 bertsioa eta aurrekoak;
- Ellipse APM, 5.2.0.3 bertsioa eta aurrekoak;
- Ellipse APM, 5.1.0.6 bertsioa eta aurrekoak.

Azalpena:

Hitachi ABB Power Grids etxeak tarteko larritasuneko ahultasun baten berri eman dio CISAri. Horren bidez, baimena lortzen duen erasotzaile batek edota aplikazio integratu batek datu maltzurrak injektatu edota kode arbitrarioa exekuta lezake.

Konponbidea:

5.3.0.2, 5.2.0.4 eta 5.1.0.7 bertsioak eguneratzea, hurrenez hurren.

Detalle:

Kaltetutako produktuen panel nagusian biltegiratutako XSS ahultasun baten bidez, baimena lortu duen erasotzaile batek edota aplikazio integratu batek datu maltzurrak injekta litzake, edota kode arbitrarioa exekutatu. Ahultasun horretarako, CVE-2021-27887 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Kodearen urruneko exekuzioa Advantech WebAccess/HMI Designer sisteman

Argitalpen data: 2021/04/22

Garrantzia: Handia

Kaltetutako baliabideak:

WebAccess/HMI Designer.

Azalpena:

9SG Security Team taldeko *kimiya* ikertzaileak 0day motako ahultasun baten berri eman du, larritasun handikoa, Advantech-en WebAccess/HMI Designer sisteman antzemandakoa.

Konponbidea:

Ahultasun hori publikoki zabaldu da, partxerik gabe, ZDIren argitalpen epearen arabera. Arintze-estrategia eraginkor bakarra aplikazioarekiko interakzioa mugatzea da.

Xehetasuna:

Ahultasuna SBF artxiboen parseoan ematen da, zehazki erabiltzaileak emandako datuen balioztatze okerra dela eta. Horren ondorioz, memoria gaiztotu liteke, eta urruneko erasotzaile batek kode arbitrarioa exekutako luke Advantech-en WebAccess/HMI Designer kaltetutako gailuetan.

Etiketak: 0day, Azpiegitura kritikoak, IoT, SCADA, Ahultasuna.

Egiaztatzearen omisioa Mitsubishi Electric GOT sisteman

Argitalpen data: 2021/04/26

Garrantzia: Tartekoa

Kaltetutako baliabideak:

Mitsubishi Electric konpainiak jakinarazi duenez, ahultasunak honako gailuen VNC funtzioari eragiten dio:

- GOT2000 series:
  - GT27 modeloa, bertsio guztiak;
  - GT25 modeloa, bertsio guztiak;
  - GT21 modeloa, bertsio guztiak;
    - GT2107-WTBD, bertsio guztiak;
    - GT2107-WTSD, bertsio guztiak.
- GOT SIMPLE series:
  - GS21 modeloa:
    - GS2110-WTBD-N, bertsio guztiak;
    - GS2107-WTBD-N, bertsio guztiak.

Azalpena:

Mitsubishi Electric konpainiak CISAri eman dio ahultasun baten berri: tarteko larritasunekoa da, eta, hori baliatuz, erasotzaile batek baimenik gabe sartzeko lortu lezake.

Konponbidea:

Mitsubishi Electric konpainiak oraindik ez du ahultasunerako partxea argitaratu. Arintze-neurri moduan, erabiltzaileei adierazi die produkturako sarbidea mugatzeko, soilik konfiantzazko *host* eta sareen bidez.

Xehetasuna:

Pasahitza egiaztatzearen omisio motako ahultasun bat dago GOT2000 seriearen eta GOT SIMPLE seriearen VNC funtzioan, egiaztatze desegoki baten ondorioz. VNC zerbitzariaren konfigurazioa aktibatuta dagoenean, erasotzaile batek baimenik gabeko sarbidea burutu lezake, bereziki diseinatutako paketeak bidaliz. Ahultasun horretarako, CVE-2021-20590 identifikatzailea esleitu da.

Etiketak: Azpiegitura kritikoak, Birtualizazioa, Ahultasuna.

Hainbat ahultasun Bosch produktuetan

Argitalpen data: 2021/04/26

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Rexroth IoT Gateway;
- ctrlX CORE Runtime, XCR-V-0108.1 bertsioa eta aurrekoak.

Azalpena:

Linuxen kernel eta sistema eragilearen liburutegietan hainbat ahultasun antzeman dira. Horien bidez, erasotzaile batek

sistema konprometitu lezake, akats bat edo kode maltzurraren exekuzioa eraginez.

Konponbidea:

- ctrlX CORE-rako, Linuxen kernelaren ahultasunak XCR-V-0108 eguneratzearen bidez esku-hartzen dira.
- ctrlX CORE sistema eragilearen liburutegien ahultasunetarako, aurreikusita bertsio eguneratu bat dago 2021eko 05erako. Jarri harremanetan zure hornitzailearekin, eguneratzeak berreskuratzeko jarraibideak lortzeko.

Arintze-neurriak aplikatzea gomendatzen da, eguneratzea eskuragarri egon arte. Hemen aurki ditzakezu: 'Akzionamendu eta kontrol elektrikoen segurtasun-gida'.

Xehetasuna:

Ahultasun kritikoak honakoei dagozkie:

- Zstandard komandoen linea erabilgarritasunean (1.4.1en aurreko bertsioak), irteera artxiboak berezko baimenekin sortzen ziren. Artxiboen baimen zuzenak (sarrerakoekin kointziditzen zutenak), bukaeran soilik ezartzen ziren. Beraz, irteera-artxiboak pertsona ez desiratuek irakurri edo idatz zitzaketen. Ahultasun horretarako, CVE-2021-24031 identifikatzailea esleitu da.
- Zstandard komandoen linea erabilgarritasunak berezko baimenak zituzten irteera-artxiboak sortzen zituen eta, justu ostean, baimen horiek mugatzen zituen. Beraz, erasotzaileek irteera-artxibo horiek irakurri edo idatz zitzaketen. Ahultasun horretarako, CVE-2021-24032 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2020-27815, CVE-2020-27830, CVE-2020-28374, CVE-2020-28941, CVE-2020-29568, CVE-2020-29569, CVE-2020-29660, CVE-2020-29661, CVE-2021-24032, CVE-2021-27218, CVE-2021-27219, CVE-2021-27803, CVE-2020-27815, CVE-2020-27830, CVE-2020-28374, CVE-2020-28941, CVE-2020-29568, CVE-2020-29569, CVE-2020-29660, CVE-2020-29661, CVE-2021-20232, CVE-2021-24031, CVE-2021-24032, CVE-2021-27218, CVE-2021-27219 eta CVE-2021-27803.

GEtiketak: Azpiegitura kritikoak, IoT, Linux, Ahultasuna.

Hainbat ahultasun Horner Automation erakundearen Cscape sisteman

Argitalpen data: 2021/04/26

Garrantzia: Handia

Kaltetutako baliabideak:

Cscape, 9.90 SP4 bertsioaren aurreko guztiak.

Azalpena:

Claroty erakundeko Sharon Brizinov ikertzaileak larritasun handiko bi ahultasunen berri eman dio CISAri. Horien bidez, erasotzaile batek pribilegioetan gora egin lezake, edota uneko prozesuan kodea exekutatu.

Konponbidea:

Cscape 9.90 SP4 bertsiora eguneratzea.

Xehetasuna:

- Erabiltzaileak proiektuaren artxiboak aztertzean emandako datuen balioztatze desegokiaren ondorioz, erasotzaile batek memoriaren ustelkeria eragin lezake, uneko prozesuaren testuinguruan kodea exekutatzeko. Ahultasun horretarako, CVE-2021-22678 identifikatzailea esleitu da.
- Berezko konfigurazioa dela eta, erabiltzaile guztiek instalatu dezakete produktua, eta horrek baimen konplexuak baimentzen ditu, idazketa/irakurketarako sarbidea barne. Hori horrela izanik, pribilegiorik gabeko erasotzaile batek artxibo bitarrak eta konfiguraziokoak aldatu litzake, pribilegioetan gora egin ahal izateko. Ahultasun horretarako, CVE-2021-22682 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun Yokogawa produktu batzuetan

Argitalpen data: 2021/04/26

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Exaopc R1.01.00 - R3.78.00;
- Exaquantum R1.10.00 - R3.20.00;
- ProSafe-RS R1.01.00 - R4.05.00. Hurrengo paketeak honakoei eragiten die:
  - RS4E5100 Safety System Engineering and Maintenance Function,
  - RS4H2200 SOE OPC Interface Package.
- CENTUM VP (Including Entry Class) R4.01.00 - R6.07.10. Hurrengo paketeak VP6P6930 SEM OPC Interface Package bertsioari eragiten dio.
- PRM R2.01.00 - R4.03.00;
- Field Wireless Device OPC Server R2.01.00, R2.01.01, R2.01.03, R2.01.10;

- STARDOM VDS R4.01 - R8.10;
- B/M9000 VP R7.01.01 - R8.03.00;
- CENTUM VP Controller FCS (Field Control Station), módulo de procesador FCS CP461 prozesadorearen modulua, FCS motak:
  - AFV30S,
  - AFV30D,
  - AFV40S,
  - AFV40D,
  - A2FV50S,
  - A2FV50D,
  - A2FV70S,
  - A2FV70D.

Azalpena:

Yokogawa erakundeak hainbat RCE produktu ahul identifikatu ditu. Microsoft Visual Basic 6.0 Runtime Extended Files sistemaren erabileraren ondoriozkoa eta alboko kanaleko erasoen ondoriozkoa da arazoa (side-channel attacks), Meltdown/Spectre ahultasunek eraginda.

Konponbidea:

Kaltetutako produktuak honako bertsioetara edo hurrengoetara eguneratzea:

- Exaopc R3.78.10;
- Exaquantum R3.20.02;
- ProSafe-RS R4.06.00;
- CENTUM VP R6.08.00 / R5.04.D3;
- PRM R4.04.00;
- Field Wireless Device OPC Server R2.01.11;
- STARDOM VDS R9.01;
- B/M9000 VP R8.03.53;
- CENTUM VP Controller FCS R6.08.00, edo, horren ordez: CP471.

Xehetasuna:

- Yokogawaren produktu batzuetan VB6 runtime bertsio zahar bat instalatu da, eta ahultasunen bidez kodearen urruneko exekuzioa gerta liteke, erabiltzaile batek bereziki kaltetutako webgune batean nabigatuko balu.
- Hainbat CENTUM VP bertsio Meltdown/Spectreren eraginpean daude, CPU anitzen hardware inplementazioei eragiten baitie.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Microsoft, Ahultasuna.

Hainbat ahultasun Moxaren NPort IA5000A Series sisteman

Argitalpen data: 2021/04/28

Garrantzia: Handia

Kaltetutako baliabideak:

- NPort IA5150A/IA5250A Series, firmware 1.4 firmware bertsioa edo aurrekoak;
- NPort IA5450A Series, 1.7 firmware bertsioa edo aurrekoak;

Azalpena:

Alexander Nochvay, Kaspersky Lab ICS CERT erakundeko ikertzaileak, 4 ahultasunen berri eman dio Moxari. Horien bidez, sarbide desegokiko kontrola gerta liteke, babesik gabeko kredentzialen biltegiratzea, edo informazio sentikorraren transmisioa.

Konponbidea:

- CVE-2020-27149 ahultasunerako, eguneratu:
  - NPort IA5150A/IA5250A Series: 1.5 *firmware* bertsiora edo ostekoetara;
  - NPort IA5450A Series: 2.0 *firmware* bertsiora edo ostekoetara.
- CVE-2020-27149 ahultasunerako: Moxaren produktuek aurrez partekatutako funtzio bat onartzen dute, konfigurazio artxiboa kodifikatu eta arrisku hori arintzeko. Kontsultatu erabiltzailearen eskuliburuko Export/Import atala xehetasun gehiago izateko.
- CVE-2020-27184 ahultasunerako: Moxa produktuek Telnet zerbitzua desaktibatu lezakete, arrisku hori arintzeko. Kontsultatu erabiltzailearen eskuliburuko Console Settings atala, atala xehetasun gehiago izateko. 1.5 firmware bertsioak edo ostekoek Telnet desgaituko dute berez, NPort IA5150A/IA5250A Series sisteman. 2.0 firmware bertsioak edo ostekoek Telnet desgaituko dute berez, NPort IA5450A Series sisteman.
- CVE-2020-27185 ahultasunerako: Moxa produktuek Moxa zerbitzua desaktibatu lezakete, arrisku hori arintzeko. Kontsultatu erabiltzailearen eskuliburuko Console Settings atala, atala xehetasun gehiago izateko.

Xehetasuna:

- Erasotzaile batek ahultasun hori baliatu lezake pribilegioetan gora egiteko edo goragoko pribilegio bat eskatzen duten eskaerak jasotzeko. Ahultasun horretarako, CVE-2020-27149 identifikatzailea esleitu da.
- Erasotzaile batek egiaztatze kredentzialak atera litzake segurua ez den komunikazio kanal baten bidez bidalitako konfigurazio-artxibo baten bidez, eta gero datu horiek Moxa zerbitzuaren bidez egiaztatzeko eta gailuaren konfigurazioak aldatzeko erabili. Ahultasun horretarako, CVE-2020-27150 identifikatzailea esleitu da.
- Erasotzaile batek transferitutako datu guztiak irakurri litzake komunikazioa Telnet bidez egiten bada, egiaztatze-kredentzialak, konfigurazio-datuak eta gailuaren bertsioa eta beste datu sentikor batzuk barne. Ahultasun

horretarako, CVE-2020-27184 identifikatzailea esleitu da.
- Erasotzaile batek bidalitako trafiko guztia irakur lezake Moxa zerbitzaria desgaitua dagoenean, egiaztatze-datuak, konfigurazio eta gailuen bertsioak eta beste datu sentikor batzuk barne. Ahultasun horretarako, CVE-2020-27185 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, SCADA, Ahultasuna.

Zerbitzu ukapena Beckhoff-en IPC Diagnostics UA Server eta TwinCAT OPC UA Server sistemetan

Argitalpen data: 2021/04/28

Garrantzia: Tartekoa

Kaltetutako baliabideak:

- TwinCAT OPC UA zerbitzaria, 2.3.0.12 bertsioa barne. Produktu hori TF6100 OPC UA sistemaren barne dago, eta 3.3.18 bertsiora arte dago kaltetuta.
- IPC Diagnostics-en UA zerbitzaria, 3.1.0.1 bertsiora arte, hori barne. Produktu hori Beckhoff-en IPC sistemetan aurrez instalatuta sartu da, baina berez desgaituta.

Azalpena:

Beckhoff Automation etxeak jakinarazi du TwinCAT OPC UA Server eta IPC Diagnostics UA Server-en bertsio batzuk ahulak direla zerbitzu ukapen motako erasoen eraginpean. Erasotzaile batek bereziki diseinatutako eskaerak bidal litzake exekuzioan dagoen OPC UA zerbitzarira, eta erantzuna emateari uztea eragin, zerbitzu ukapena eraginez.

Konponbidea:

- CX8091-erako, Beckhoff-ek "CX8091_CE600_LF_v356f_TC211R3_B2306_v2" firmware bertsiora edo osteko batera eguneratzea gomendatzen du.
- Windows CE exekutatzen duten gailuetarako, Beckhoff-ek gomendatzen du euskarri teknikoaren bidez irudi berri bat eskatzea.
- Windowsen beste bertsio batzuk exekutatzen dituzten gainerako gailuetarako, Beckhoff-ek gomendatzen du OPC UA zerbitzarietan bertsio berri bat lortzea, deskarga kanal ofizialen bidez.

Xehetasuna:

QI-ANXIN Technology Group taldeko Kontrol Industrialeko Segurtasun Laborategiko ikertzaileek Beckhoff fabrikatzaileari jakinarazi zioten ahultasun bat antzeman zutela. Horren bidez, erasotzaile batek TCP konexioa ezarri lezake kaltetutako OPC UA zerbitzarietako batekin, eta datu-pakete batzuk bidali, bereziki diseinatuak, OPC UA zerbitzarirako sarbide balioztatze oker baten ondoriozko pila gainezkatze bat eraginez. Horrela, administrariak eten eta berrabiarazi egin beharko luke. Ahultasun horretarako, CVE-2020-12526 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, SCADA, Ahultasuna.

Hainbat ahultasun Codesys produktu batzuetan

Argitalpen data: 2021/04/29

Garrantzia: Handia

Kaltetutako baliabideak:

CVE-2021-29242:

- CODESYS V3 produktu guztien aldagaiak, CmpChannelServer, CmpChannelServerEmbedded, CmpRouter edo CmpRouterEmbedded osagaia duten 5.17.0 bertsioaren aurreko guztietan, CPU mota edo sistema eragilea edozein dela ere:
  - CODESYS Control RTE V3,
  - CODESYS Control RTE V3 (para Beckhoff CX),
  - CODESYS Control Win V3,
  - CODESYS Control V3 Runtime System Toolkit,
  - CODESYS V3 Embedded Target Visu Toolkit,
  - CODESYS V3 Remote Target Visu Toolkit,
  - CODESYS V3 Safety SIL2,
  - CODESYS Edge Gateway Windows-erako
  - CODESYS Gateway V3,
  - CODESYS HMI V3,
  - CODESYS OPC Server V3,
  - CODESYS PLCHandler SDK,
  - CODESYS V3 Simulation Runtime (CODESYS Development System sistemaren parte).
- CODESYS Control V3 Runtime System Toolkit sisteman oinarritutako produktu hauek 4.1.0.0 bertsioaren aurreko bertsio guztiak kaltetuak daude:
  - CODESYS Control BeagleBone SL,-erako,
  - CODESYS Control emPC-A/iMX6 SL,-erako,
  - CODESYS Control IOT2000 SL,-erako,
  - CODESYS Control Linux SL,-erako,
  - CODESYS Control Linux ARM SL,-erako,

- CODESYS Control PLCnext SL, -erako,
- CODESYS Control PFC100 SL, -erako,
- CODESYS Control PFC200 SL, -erako,
- CODESYS Control Raspberry Pi SL, -erako,
- CODESYS Control WAGO Touch Panels 600 SL, -erako,
- CODESYS Edge Gateway Linux-erako.

CVE-2021-29240 eta CVE-2021-29239: 3.5.17.0 bertsioaren aurreko CODESYS Development System V3 bertsio guztiak, 32 bit-erakok eta 64 bit-ekoak.

CVE-2021-29241:

- CmpGateway osagaia duten CODESYS V3 produktu hauen aldagai guztiak, CPU edo sistema eragilea edozein dela ere:
  - CODESYS Edge Gateway, Linux-erako (4.1.0.0 bertsioaren aurreko kaltetutako guztiak);
  - CODESYS Control V3 Runtime System Toolkit (3.5.17.0 bertsioaren aurreko kaltetutako guztiak);
  - CODESYS Development System (3.5.17.0 bertsioaren aurreko kaltetutako guztiak);
  - CODESYS Edge Gateway, Windows-erako (3.5.17.0 bertsioaren aurreko kaltetutako guztiak);
  - CODESYS Gateway V3 (3.5.17.0 bertsioaren aurreko kaltetutako guztiak).
- *CmpGateway* ezabatu egin zen ondoren azaldutako bertsioak zituzten produktuetatik. Beraz, produktu hauen bertsio berrienak ez daude kaltetuta:
-
  - CODESYS Control, BeagleBone SL-rako (4.0.1.0 bertsioaren aurreko kaltetutako guztiak);
  - CODESYS Control, emPC-A/iMX6 SL-rako (4.0.1.0 bertsioaren aurreko kaltetutako guztiak);
  - CODESYS Control, IOT2000 SL-rako (4.0.1.0 bertsioaren aurreko kaltetutako guztiak);
  - CODESYS Control, Linux-erako (4.0.1.0 bertsioaren aurreko kaltetutako guztiak);
  - CODESYS Control, PFC100 SL-rako (3.5.16.0 bertsioaren aurreko kaltetutako guztiak);
  - CODESYS Control, PFC200 SL-rako (3.5.16.0 bertsioaren aurreko kaltetutako guztiak);
  - CODESYS Control, Raspberry Pi SL -erako (4.0.1.0 bertsioaren aurreko kaltetutako guztiak).

CVE-2021-29238: 1.16.0 bertsioaren aurreko CODESYS Automation Server bertsioak kaltetuta daude. CODESYS GmbH sistemak zuzenketa-bertsio honetara eguneratu ditu instantzia guztiak.

Azalpena:

Hainbat ikertzailek larritasun handiko 5 ahultasunen berri eman diote Codesys erakundeari. Horiek baliatzearen ondorioz, erasotzaile batek maila baxuko komunikazio-paketeak alda litzake, pakete maltzurrak instalatu, artxibo maltzurrak editatu edota exekutatu, DoS baldintza eragin edo pribilegioetan gora egin.

Konponbidea:

CVE-2021-29242

- CODESYS GmbH eguneratzea 3.5.17.0 bertsiora, honako produktuetako ahultasuna konpontzeko:
  - CODESYS Control RTE V3,
  - CODESYS Control RTE V3 (Beckhoff CX-rako),
  - CODESYS Control Win V3,
  - CODESYS Control V3 Runtime System Toolkit,
  - CODESYS V3 Embedded Target Visu Toolkit,
  - CODESYS V3 Remote Target Visu Toolkit,
  - CODESYS V3 Safety SIL2,
  - CODESYS Edge Gateway Windows-erako,
  - CODESYS Gateway V3,
  - CODESYS HMI V3,
  - CODESYS OPC Server V3,
  - CODESYS PLCHandler SDK,
  - CODESYS V3 Simulation Runtime (CODESYS Development System-aren parte).
- Ahultasuna 4.1.0.0 bertsioarekin konponduko da (horren argitalpena 2021eko maiatzerako planeatuta dago), CODESYS Control V3 Runtime System Toolkit V3.5.17.0 bertsioan oinarritua;
  - CODESYS Control, BeagleBone SL-rako,
  - CODESYS Control, emPC-A/iMX6 SL-erako,
  - CODESYS Control, IOT2000 SL-erako,
  - CODESYS Control, Linux SL-rako,
  - CODESYS Control, Linux ARM SL-rako,
  - CODESYS Control, PLCnext SL-erako,
  - CODESYS Control, PFC100 SL-erako,
  - CODESYS Control, PFC200 SL-erako,
  - CODESYS Control, Raspberry Pi SL-rako,
  - CODESYS Control, WAGO Touch Panels 600 SL-rako,
  - CODESYS Edge Gateway, Linux-erako.

CVE-2021-29240 eta CVE-2021-29239: CODESYS GmbH sistemak 3.5.17.0 bertsioa abiarazi du, ahultasun horiek konpontzeko.

CVE-2021-29241:

- CODESYS GmbH sistemak 3.5.17.0 bertsioa abiarazi du, honako produktuetan ahultasun konpontzeko:
  - CODESYS Control V3 Runtime System Toolkit,
  - CODESYS Gateway V3,
  - CODESYS Development System,
  - CODESYS Edge Gateway Windows-erako.
- CODESYS Edge Gateway-ren kasuan, ahultasuna 4.1.0.0 bertsioarekin konponduko da (horren argitalpena 2021eko maiatzerako planeatuta dago), CODESYS Control V3 Runtime System Toolkit V3.5.17.0 bertsioan oinarritua

CVE-2021-29238: CODESYS GmbH sistemak 1.16.0 bertsiora eguneratu ditu CODESYS Automation Server instantzia guztiak.

Xehetasuna:

- Urruneko erasotzaile batek bereziki diseinatutako komunikazio-paketeak bidal litzake, routerren bideratze eskema

aldatzeko eta bezeroen eta CODESYS Control exekuzio sistemaren artean maila baxuko komunikazio paketeak desbideratu, gehitu, ezabatu edo aldatzeko. Ahultasun horretarako, CVE-2021-29242 identifikatzailea esleitu da.
- CODESYS Development System sistemaren pakete-kudeatzaileak ez du paketeen baliagarritasuna konprobatzen instalazioaren aurretik, eta tokiko eduki maltzurra duten CODESYS paketeak instalatzeko erabil liteke. Ahultasun horretarako, CVE-2021-29240 identifikatzailea esleitu da.
- CODESYS Development System sistemak liburutegietan sartutako artxibo edo dokumentu maltzurrak erakutsi edo exekutatzen ditu, aldez aurretik baliagarritasuna konprobatu aurretik. Ahultasun horretarako, CVE-2021-29239 identifikatzailea esleitu da.
- Bereziki diseinatutako komunikazio eskaerek puntero nuluaren erreferentzia eza eragin lezakete (null pointer dereference) hainbat CODESYS produktutan, eta horrek zerbitzuaren ukapena eragin lezake (DoS), urruneko erasotzaile batek egina. Ahultasun horretarako, CVE-2021-29241 identifikatzailea esleitu da.
- Kontroladore batean zabaldutako CODESYS Web Visualization baten artxiboak manipulatuko lituzkeen urruneko erasotzaile batek pribilegioetan gora egitea eragin lezake, Web Visualization CODESYS Automation Server-ekin irekitzen denean. Ahultasun horretarako, CVE-2021-29238 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Artxiboen irakurketa arbitrarioa Cassia Networks-en Access Controller sisteman

Argitalpen data: 2021/04/30

Garrantzia: Tartekoa

Kaltetutako baliabideak:

Access Controller, 2.0.1 bertsioaren aurreko guztiak.

Descripción:

Azalpena:

Amir Preminger eta Sharon Brizinov, Claroty erakundeko ikertzaileek, ahultasun baten berri eman diote CISAri. Tarteko larritasunekoa da, direktorio mugaturako mugatze desegokiaren motakoa, eta Cassia Networks-en Access Controller produktuari eragiten dio.

Konponbidea:

Cassia Networks-ek partxe bat argitaratu du (saioa hasi beharra dago), emandako ahultasuna zuzentzen duena.

Xehetasuna:

Erasotzaile batek *minify i*bilbidea erabili lezake, ibilbide erlatiboarekin, Access Controller zerbitzarian edozein artxibo ikusteko. Ahultasun horretarako, CVE-2021-22685 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun Texas Instruments SimpleLink produktuetan

Argitalpen data: 2021/04/30

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SimpleLink MSP432E4 SDK, v4.20.00.12 bertsioa eta aurrekoak;
- SimpleLink CC32XX SDK, v4.30.00.06 bertsioa eta aurrekoak;
- SimpleLink CC13X0 SDK, v4.10.03 bertsioaren aurrekoak;
- SimpleLink CC13X2 SDK, v4.40.00 bertsioaren aurrekoak;
- SimpleLink CC26XX SDK, v4.40.00 bertsioaren aurrekoak;
- CC3200 SDK, v1.5.0 bertsioa eta aurrekoak;
- CC3100 SDK, v1.3.0 bertsioa eta aurrekoak.

Azalpena:

Microsoft erakundeko David Atch eta Omri Ben Bassat ikertzaileek ahultasun horien berri eman diote CISAri. Horien bidez, erasotzaile batek zerbitzu ukapena edota kodearen urruneko exekuzioa burutu litzake.

Konponbidea:

Azken software bertsioetara eguneratzea.

Xehetasuna:

- Host-aren MCUaren APIan osoen gainezkatzea izanez gero, wifi sare batera konektatzeko saiakeran, erasotzaile batek zerbitzu ukapena edota kodearen exekuzioa eragin litzake. Ahultasun horretarako, CVE-2021-22677 identifikatzailea esleitu da.
- CDN zerbitzaritik firmware over-the-air eguneratzeak prozesatzen diren bitartean pilan oinarritutako bufferraren

gainezkatzea gertatuz gero, erasotzaile batek kodearen urruneko exekuzioa burutu lezake. Ahultasun horretarako, CVE-2021-22677 identifikatzailea esleitu da.
- Firmware over-the-air eguneratze-artxiboak aztertzean osoen gainezkatzea gertatzearen ondorioz, erasotzaile batek kodearen urruneko exekuzioa burutu lezake. Ahultasun horretarako, CVE-2021-22675 identifikatzailea esleitu da.
- HTTP goiburuak prozesatzean osoen gainezkatzea gertatzearen ondorioz, erasotzaile batek kodearen urruneko exekuzioa burutu lezake. Ahultasun horretarako, CVE-2021-22679 identifikatzailea esleitu da.
- Domeinu-izen luzeak prozesatzean osoen gainezkatze batzuk gertatzearen ondorioz, erasotzaile batek kodearen urruneko exekuzioa burutu lezake. Ahultasun horretarako, CVE-2021-22671 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun sistema eragileetan, denbora errealean (RTOS)

Argitalpen data: 2021/04/30

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Amazon FreeRTOS, 10.4.1 bertsioa;
- Apache Nuttx OS, 9.1.0 bertsioa;
- ARM CMSIS-RTOS2, 2.1.3 bertsioaren aurrekoak;
- ARM Mbed OS, 6.3.0 bertsioa;
- ARM mbed-uallaoc, 1.3.0 bertsioa;
- Software Cesanta Mongoose OS, v2.17.0 bertsioa;
- eCosCentric eCosPro RTOS, 2.0.1etik 4.5.3ra bitarteko bertsioak;
- Google Cloud IoT gailuaren SDK, 1.0.2 bertsioa;
- Linux Zephyr RTOS, 2.4.0 bertsioaren aurrekoak;
- Media Tek LinkIt SDK, 4.6.1 bertsioaren aurrekoak;
- Micrium OS, 5.10.1 bertsioa eta aurrekoak;
- Micrium uCOS II / uCOS III 1.39.0 bertsioak eta aurrekoak;
- NXP MCUXpresso SDK, 2.8.2 bertsioaren aurrekoak;
- NXP MQX, 5.1 bertsioa eta aurrekoak;
- Redhat newlib, 4.0.0 bertsioaren aurrekoak;
- RIOT OS, 2020.01.1 bertsioa;
- Samsung Tizen RT RTOS, 3.0.GBB bertsioaren aurrekoak;
- TencentOS-tiny, 3.1.0 bertsioa;
- Texas Instruments CC32XX, 4.40.00.07 bertsioaren aurrekoak;
- Texas Instruments SimpleLink MSP432E4XX;
- Texas Instruments SimpleLink-CC13XX, 4.40.00 bertsioaren aurrekoak;
- Texas Instruments SimpleLink-CC26XX, 4.40.00 bertsioaren aurrekoak;
- Texas Instruments SimpleLink-CC32XX, 4.10.03 bertsioaren aurrekoak;
- Uclibc-NG, 1.0.36 bertsioaren aurrekoak;
- Windriver VxWorks, 7.0 bertsioaren aurrekoak.

Azalpena:

Hainbat ahultasun antzeman dira fabrikatzaile askoren sistema eragileetan denbora errealean (RTOS), memoriaren esleipen funtzioen erabilerarekin erlazionatutako ahultasun multzo baten ondorioz, hala nola malloc, calloc, realloc, memalign, valloc, pvalloc, eta abar. Horiek guztiak 'BadAlloc' izeneko txosten baten bidez ezagutarazi dira. Ahultasun horien bidez, erasotzaile batek kodearen urruneko exekuzioa burutu lezake, edota kaltetutako gailuaren blokeoa eragin.

Konponbidea:

- Amazon FreeRTOS: eguneratzea deskargatu;
- Apache Nuttx OS 9.1.0 bertsioa: eguneratzea deskargatu;
- ARM CMSIS-RTOS2: eguneratzea bidean, ekainerako aurreikusia;
- ARM Mbed OS: eguneratzea deskargatu;
- ARM mbed-uallaoc: Sistema zaharkitua da eta ez da eguneratzerik egingo;
- Cesanta Software mongooses: eguneratzea deskargatu;
- eCosCentric eCosPro RTOS: Eguneratzea: 4.5.4 bertsioak eta ostekoak;
- Google Cloud IoT gailuen SDK: eguneratzea deskargatu;
- Media Tek LinkIt SDK: MediaTek erakundeak erabiltzaileei eskainiko die eguneratzea. Ez dago konponbiderik doako bertsiorako, izan ere, ez dago diseinatuta produkzio-erabilerarako;
- Micrium OS: Eguneratzea: 5.10.2 bertsioa edo ostekoa;
- Micrium uCOS-II / uCOS-III: 1.39.1 bertsiora eguneratzea: Eguneratzea oraindik argitaratu gabe;
- NXP MCUXpresso SDK: Eguneratzea: 2.9.0 bertsioa edo ostekoa;
- NXP MQX: Eguneratzea: 5.1 edo ostekoa;
- Redhat newlib: eguneratzea deskargatu;
- RIOT OS: eguneratzea deskargatu;
- Samsung Tizen RT RTOS: eguneratzea deskargatu;
- TencentOS-tiny: Eguneratzea deskargatu;
- Texas Instruments CC32XX: v4.40.00.07 bertsiora eguneratzea;
- Texas Instruments SimpleLink CC13X0: v4.10.03 bertsiora eguneratzea; eguneratzea argitaratu gabe;
- Texas Instruments SimpleLink CC13X2-CC26X2: v4.40.00 bertsiora eguneratzea; eguneratzea argitaratu gabe;
- Texas Instruments SimpleLink CC2640R2: v4.40.00 bertsiora eguneratzea; eguneratzea argitaratu gabe;
- Texas Instruments SimpleLink MSP432E4: konfirmatua. Egun ez dago eguneratzerik planifikatuta;
- uClibc-ng: eguneratzea deskargatu;
- Windriver VxWorks: Eguneratzea bidean.

Gainera, CISAk kaltetutako erabiltzaileei honako arintze-neurriak gomendatu dizkie:

- Murriztu sarearen eragin-eremua gailu guztietan, bereziki, Internet bidezkoa.
- Kokatu kontrol-areak eta urrutiko gailuak firewall babesen atzean, eta enpresa-saretik aparte.
- Urrutiko sarbidea behar denean, erabili metodo seguruak, hala nola sare pribatu birtualak (VPN).

Xehetasuna:

Microsofteko 52 Atalaren taldeko David Atch, Omri Ben Bassat eta Tamir Ariel ikertzaileek, IoT-erako Azure Defenser segurtasun-talde gisa, hainbat ahultasun kritikoren multzoa antzeman dute. IoT eta OT gailuetako memoria esleipenari eragiten diote. 'BadAlloc' izeneko ahultasun horiek memoriaren esleipen funtzio estandarrei eragiten diete. Horien barruan daude hainbat fabrikatzaileren denbora errealeko sistema eragileak (RTOS), software garapenerako kit integratuak (SDK) eta estandar liburutegien inplementazio estandarrak (libc).

Aurkitutako ahultasunak memoria esleitzeko funtzio ahulei eragiten diete, hala nola malloc, calloc, realloc, memaling, valloc, pvalloc, eta abar. Kaltetutako produktuen funtzio horien inplementazioak ez ditu sarbide-balioztatze egokiak gehitu. Sarbide-balioztatze horiek gabe, erasotzaile batek memoria esleipena baliatu lezake pilaren gainezkatzea burutzeko, eta horrek gailuan kode maltzurra exekutatzea ekarriko luke.

Ahultasun horiei honako identifikatzaileak esleitu zaizkie: CVE-2021-30636, CVE-2021-27431, CVE-2021-27433, CVE-2021-27435, CVE-2021-27427, CVE-2021-22684, CVE-2021-27439, CVE-2021-27425, CVE-2021-26461, CVE-2020-35198, CVE-2020-28895, CVE-2021-31571, CVE-2021-31572, CVE-2021-27417, CVE-2021-3420, CVE-2021-27411, CVE-2021-26706, CVE-2021-27421, CVE-2021-22680, CVE-2021-27419, CVE-2021-27429, CVE-2021-22636, CVE-2021-27504 eta CVE-2021-27502.

Etiketak: Eguneratzea, Apache, Komunikazioak, Azpiegitura kritikoak, IoT, Linux, Ahultasuna.

Pribilegioen eskalatzea Johnson Controls produktuetan

Argitalpen data: 2021/04/30

Garrantzia: Handia

Kaltetutako baliabideak:

- Serie Z eta Serie A Linuxen oinarrituak,
- Q Seriea,
- G Seriea,
- LC serie heredatua,
- ELP serie heredatua,
- Bideo-grabagailuak exacqVision (NVR) sarean,
- Linuxen oinarritutako C serieko lan-estazioak,
- S serieko biltegiratze-zerbitzariak.

Azalpena:

Johnson Controls erakundeak ahultasunaren berri eman dio CISAri. Horren bidez, erasotzaile batek pribilegioen eskalatzea burutu lezake

Konponbidea:

Johnson Controls erakundeak erabiltzaileei gomendatu die Ubuntu Linux sistema eragilearen azken segurtasun eguneratzeak instalatzeko.

Xehetasuna:

exacqVision izeneko sareko bideo-grabagailuaren bertsioetan izandako ahultasun batzuek, Ubuntu Linux sistema eragilean erabiliak, Sudo aplikazio integratuari eragiten diote. Horrek supererabiltzailearen sistema eragilerako sarbide-hornidura kontrolatzen du (administraria). Horrela izanik, erasotzaile batek supererabiltzailearen pribilegioen eskalatzea burutu lezake, baimenik gabe, azpiko Ubuntu sistema eragilera. Ahultasun horretarako, CVE-2021-3156 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, Linux, Ahultasuna.