2020ko Ekainaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Buferrak gainezka egitea: Point-to-Point Protocol Daemon

Argitalpen data: 2020/06/02

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Demonio pppd (*Point to Point Protocol Daemon*), 2.4.2 bertsiotik 2.4.8 bertsiora.

- Kaltetutako fabrikatzaileak:
  - Phoenix Conctac:
    - FL MGUARD, TC MGUARD, TC ROUTER eta TC CLOUD CLIENT gailuak.

Deskripzioa:

IOActive etxeko Ilja Van Sprundel ikertzaileak demonio pppd sistemari eragiten dion ahultasun kritiko bat atzeman du. Egiaztatu gabeko urrutiko erasotzaile batek buferrak gainezka egitea eragin dezake, eta, horrela, sisteman kode arbitrario bat exekutatu.

Konponbidea:

Eskuragarri dagoen azken pppd partxea aplikatzea, horretan dauden konfigurazioen arabera. Informazio gehiago izateko, kontsultatu Erreferentzien atala.

Xehetasuna:

Demonio pppd sistemako *Extensible Authentication Protocol* (EAP) paketeen prozesatzearen akats baten ondorioz, egiaztatu gabeko urruneko erasotzaile batek buferrak gainezka egitea eragin dezake, eta sisteman kode arbitrario bat exekutatu lezake. Ahultasun horretarako, CVE-2020-8597 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna

Funtzio kritikoaren egiaztapen falta Grid Solutions Reason RT Clocks erakundean

Argitalpen data: 2020/06/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Grid Solutions Reason RT Clocks RT430, RT431 eta RT434, 08A05 bertsioaren aurreko *firmware* bertsio guztiak.

Deskripzioa:

IOActive-ko Ehab Husseinek ahultasun kritiko baten berri eman zion GE fabrikatzaileari. Egiaztatze falta arloko ahultasuna somatu zuen Grid Solutions Reason RT Clocks markaren hainbat bertsiotan.

Konponbidea:

Fabrikatzaileak gomendatu du kaltetutako produktuen *firmware* bertsioa 08A05era eguneratzea.

Xehetasuna:

Ahultasun horren ondorioz, egiaztatu gabeko erasotzaile batek komando arbitrarioak exekutatu litzake eta URL espezifiko batera eskaera

bat bidali. Horrela, gailuak erantzuteari utziko lioke. Erabiltzailearen configuration kontuaren pasahitza aldatu lezake, horrela, gailuaren *konfigurazioa* aldatu ahal izango luke web interfazearen bidez, pasahitz berria erabiliz, edo eskatutako egiaztatzea alde batera utziko litzateke gailua konfiguratu eta sistema berrabiarazteko. Ahultasun horretarako, CVE-2020-12017 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Pasahitzen kudeaketa desegokia PACTware produktuetan

Argitalpen data: 2020/06/03

Garrantzia: Handia

Kaltetutako baliabideak:

PACTware, bertsioak:

- 5.0.4.xx eta aurrekoak;
- 4.1 SP5 eta aurrekoak;
- 3.X eta aurrekoak;
- 2.4 eta aurrekoak;

Deskripzioa:

Dragos Inc konpainiako Reid Wightmanek, eta BSI erakundeek koordinatuta, bi ahultasunen berri eman du kaltetutako produktuen pasahitzen kudeaketaren inguruan.

Konponbidea:

PACTware 5.0.5.31, PACTware 4.1 SP6 edo goragoko bertsioak eguneratzea.

Xehetasuna:

PACTware markak aukera ematen du "erabiltzaile rolak" erabiltzeko, FDT zuzentarauen araberako sarbidea mugatuz. Hala ere, berez ez da pasahitzik ezartzen, eta erabiltzaileak administrari rola dauka, inolako mugarik gabe.

Erabiltzaileak rolen sarbide-kontrola gaitzen badu, rol bakoitza pasahitz indibidual baten bidez babestu daiteke.

- Doikuntza horiek tokiko erabiltzaile batek aldatu ditzake inolako egiaztatzerik gabe, eta horren ondorioz rolaren habilitazioa aldatzeko aukera egon daiteke, baita rolen pasahitzak ere, aldez aurretik ezer egiaztatu beharrik gabe. Ahultasun horretarako, CVE-2020-9404 identifikatzailea erreserbatu da.
- Doikuntzak egiaztatu gabeko tokiko erabiltzaile batek irakur ditzake. Posible da rolen pasahitzak berreskuratzea, pasahitzak aldez aurretik ezarritakoak badira. Ahultasun horretarako, CVE-2020-9403 identifikatzailea erreserbatu da.

Erabiltzaileak ez baditu banakako rolak gaitu, erasotzaile batek rol horiek habilitatu eta pasahitzak eman ahalko lizkieke. Horren ondorioz, benetako erabiltzaileek *softwarea* erabiltzen dute.

Etiketak: Eguneraketa, Ahultasuna

Moxa-ren VPort461 sistemako komandoen injekzioa

Argitalpen data: 2020/06/08

Garrantzia: Handia

Kaltetutako baliabideak:

Vport 461 gailuak, 3.4 firmware bertsioarekin edo hortik beherakoarekin.

Deskripzioa:

Beijin Chaitin Future Technology Co., Ltd erakundeko Xinjie Ma ikertzaileak , Komandoen injekzio motako ahultasun baten berri eman zuen; VPort 461 Series Industrial Video Servers gailuei eragiten die.

Konponbidea:

Moxak kaltetutako bezeroei eskatu die laguntza teknikoko zerbitzuarekin harremanetan jartzeko, arazo konpontze aldera.

Xehetasuna:

Gailuaren ahultasun baten ondorioz, urrutiko erasotzaile batek komando arbitrarioak exekutatu litzake.

Etiketak: Eguneratzea, Ahultasuna

Buferrak gainezka egitea Advantech WebAccess Node sisteman

Argitalpen data: 2020/06/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Advantech WebAccess Node, 8.4.4 bertsioa eta aurrekoak.

Deskripzioa:

Z0mb1E erakundeak, Trend Micro-ren Zero Day Initiative ekimenaren barruan, larritasun kritikoko ahultasun baten berri eman zion CISAri, pilan oinarritutako bufer gainezkatzearen arlokoa (*stack*).

Konponbidea:

Fabrikatzaileak P0520844 partxea argitaratu du ahultasun hori konpontzeko.

Xehetasuna:

Kaltetutako produktuari pilan oinarritutako bufer gainezkatzeak eragin ahal dio (stack). Horrela, urrutiko erasotzaile batek kode arbitrarioa exekutatu lezake. Ahultasun horretarako, CVE-2020-12019 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Siemensen segurtasun buletina. 2020ko ekaina

Argitalpen data: 2020/06/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- LOGO!8 BM (SIPLUS aldaerak barne), bertsio guztiak;
- SIMATIC Automation Tool, bertsio guztiak;
- SIMATIC NET PC software, v16-tik aurrerako bertsio guztiak, v16 Upd3-ren aurrekoak;
- SIMATIC PCS 7, bertsio guztiak;
- SIMATIC PCS neo, bertsio guztiak;
- SIMATIC ProSave, bertsio guztiak;
- SIMATIC S7-1500 Software Controller, bertsio guztiak;
- SIMATIC STEP 7, v5.6 SP2 HF3 bertsioaren aurreko guztiak;
- SIMATIC STEP 7 (TIA Portal) v13, bertsio guztiak;
- SIMATIC STEP 7 (TIA Portal) v14, bertsio guztiak;
- SIMATIC STEP 7 (TIA Portal) v15, bertsio guztiak;
- SIMATIC STEP 7 (TIA Portal) v16, bertsio guztiak;
- SIMATIC WinCC OA v3.16, P018-ren aurreko bertsio guztiak;
- SIMATIC WinCC OA v3.17, P003-ren aurreko bertsio guztiak;
- SIMATIC WinCC Runtime Professional v13, bertsio guztiak;
- SIMATIC WinCC Runtime Professional v14, bertsio guztiak;
- SIMATIC WinCC Runtime Professional v15, bertsio guztiak;
- SIMATIC WinCC Runtime Professional v16, bertsio guztiak;
- SIMATIC WinCC v7.4, v7.4 SP1 Update 14-ren aurreko bertsio guztiak;
- SIMATIC WinCC v7.5, v7.5 SP1 Update 3-ren aurreko bertsio guztiak;
- SINAMICS Startdrive, bertsio guztiak;
- SINEC NMS, bertsio guztiak;
- SINEMA Server, bertsio guztiak;
- SINUMERIK ONE virtual, bertsio guztiak;
- SINUMERIK Operate, bertsio guztiak;
- SIMATIC PDM, bertsio guztiak;
- SIMATIC STEP 7 v5.X, 5.6 SP2 HF3 bertsioaren aurreko guztiak;
- SINAMICS STARTER (STEP 7 OEM barne), 5.4 HF1 bertsioaren aurreko guztiak;
- SINUMERIK Access MyMachine/P2P, 4.8 bertsioaren aurreko guztiak;
- SINUMERIK PCU base Win10 software/IPC, 14.00 bertsioaren aurreko guztiak;
- SINUMERIK PCU base Win7 software/IPC, 12.01 HF4 bertsioaren aurreko guztiak;

Deskripzioa:

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

Konponbidea:

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

Xehetasuna:

Siemensek, segurtasun partxeei buruzko hileroko jakinarazpenean, 7 segurtasun-abisu eman ditu; horietatik 3 eguneratzek dira.

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Funtzio kritikoko egiaztatze-gabeziaren ahultasun bat,
- Komatxo artena sartu gabeko bilaketa-elementu edo ibilbidearen ahultasuna,
- Komatxo artean sartu gabeko bilaketa-elementu edo ibilbidearen ahultasuna,
- Memoria dinamikoan oinarritutako bufer gainezkatzearen arloko 6 ahultasun (Heap),
- Pilan oinarritutako bufer gainezkatzearen 4 ahultasun (Stack),
- Mugaz kanpoko irakurketaren 4 ahultasun,
- Hasiera desegokiko 2 ahultasun,
- Buferraren amaierako memoria-kokapen batera sartzeko 3 ahultasun,
- Buferra hasi aurretik memoria kokapen baten erreferentziazko ahultasun bat,
- Luzeraren kalkuluaren errore arloko 2 ahultasun, unitate baten faltagatik edo gehiegi izateagatik (off-by-one),
- Null amaiera okerraren arloko ahultasun bat.

Ahultasun horietarako, honako identifikatzaileak erreserbatu dira: CVE-2020-7589, CVE-2020-7580, CVE-2020-7585, CVE-2020-7586, CVE-2018-15361, CVE-2019-8258, CVE-2019-8259, CVE-2019-8260, CVE-2019-8261, CVE-2019-8262, CVE-2019-8263, CVE-2019-8264, CVE-2019-8265, CVE-2019-8266, CVE-2019-8267, CVE-2019-8268, CVE-2019-8269, CVE-2019-8270, CVE-2019-8271, CVE-2019-8272,

CVE-2019-8273, CVE-2019-8274, CVE-2019-8275, CVE-2019-8276, CVE-2019-8277 eta CVE-2019-8280.

Etiketak: Eguneratzea, Siemens, Ahultasuna

Schneider Electric erakundearen segurtasun buletina. 2020ko ekaina

Argitalpen data: 2020/06/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Modicon M218, *firmware* 4.3 bertsioa eta aurrekoak;
- Unity Loader, bertsio guztiak;
- OS Loader, bertsio guztiak;
- Modicon LMC078 Logic Controller, *firmware* 1.51.15.05 bertsioa eta ostekoak.

Deskripzioa:

CNCERT erakundeak eta DingXiang Dongjian Security Lab enpresako Yang Dong ikertzaileak larritasun kritiko, altu eta ertaineko 3 ahultasun batzuen berri eman diote Schneider Electric etxeari. Arlo hauetakoak dira, hurrenez hurren: kredentzial argiak erabiltzea, puntero baliogabearen erreferentzia galtzea eta mugez kanpoko idazketa.

Konponbidea:

Fabrikatzailearen abisu bakoitzeko *Remediation / Available Remediations* atalean azaldutako eguneratze eta konfigurazio jarraibideei kasu egitea.

Xehetasuna:

Erasotzaile batek, ahultasun horiek baliatuz, honako ekintzaren bat burutu lezake:

- Modicon PLC sistemek emandako artxiboen transferentzia zerbitzura baimenik gabe sartzea;
- 2019an sortutako IPNET CVE de VxWorks 6.8.3 partxeen IGMP osagaiak puntero baliogabearen erreferentzia dauka.
- Zerbitzua ukatzea TCP/IP pakete espezifikoak bidaltzen direnean, bereziki diseinatuta, Modicon M218 kontrolatzaile logikora.

Ahultasun horietarako, honako identifikatzaileak erreserbatu dira: CVE-2020-7498 eta CVE-2020-7502, eta CVE-2020-10664 esleitu da.

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

Pribilegioen kudeaketa desegokia hainbat WAGO produktutan

Argitalpen data: 2020/06/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Honako produktuen *firmware* bertsio guztiak:

- PFC100 serieak (750-81xx/xxx-xxx),
- PFC200 serieak (750-82xx/xxx-xxx),
- 762-4xxx Wago Touch Panel 600 Standard Line,
- 762-5xxx Wago Touch Panel 600 Advanced Line,
- 762-6xxx Wago Touch Panel 600 Marine Line.

Deskripzioa:

Cisco Talos enpresako Kelly Leuschner ikertzaileak, erakundeak koordinatuta, pribilegioen kudeaketa desegokiaren arloko ahultasun kritiko bat atzeman du hainbat WAGO produktutan. Fabrikatzaileari horren berri eman dio.

Konponbidea:

WAGO produktuen aurreko esku-liburuen bertsioetan, WBM eta Linux sistemaren arteko bereizketa bat egin zen. Informazio hori ez zen zuzena, eta WAGOk eskuliburuetako egungo bertsioetan zuzendu du. 2020ko ekainean eguneratuko dira. Bertsio honetatik aurrera da baliagarria: *firmware* 03.04.10 (16) / 5.1.2.1.2. kapitulua.

Xehetasuna:

WBM (*Web Based Management*) sistemara sarbidea daukan egiaztatutako erasotzaile batek software kargaren funtzionalitatea erabil lezake *root* pribilegioak dituen software pakete bat instalatzeko. Horrela izanik, gailua manipulatu edo horren kontrola bereganatu ahal izango luke. Ahultasun horretarako, CVE-2020-6090 identifikatzailea erreserbatu da.

Etiketak: Azpiegitura kritikoak, Ahultasuna

Hainbat ahultasun Rockwell Automation-en zenbait produktutan

Argitalpen data: 2020/06/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- FactoryTalk Linx, 6.00, 6.10 eta 6.11 bertsioak;
- RSLinx Classic, 4.11.00 bertsioa eta lehenagokoak;
- FactoryTalk Linx Software erabiltzen duten ondoko produktuak:
  - Connected Components Workbench, 12 bertsioa eta lehenagokoak;
  - ControlFLASH, 14 bertsioa eta lehenagokoak;
  - ControlFLASH Plus, 1 bertsioa eta ondorengoak;
  - FactoryTalk Asset Centre, 9 bertsioa eta ondorengoak;
  - FactoryTalk Linx CommDTM, 1 bertsioa eta ondorengoak;
  - Studio 5000 Launcher, 31 bertsioa eta ondorengoak;
  - Studio 5000 Logix Designer software, 32 bertsioa eta ondorengoak.

Azalpena:

Claroty-ko Sharon Brizinov eta Amir Preminger-en 4 ahultasunen berri eman diote CISAri eta Rockwell Automationi, 2 larritasun kritikokoak eta 2 altukoak. Era hauetakoak dira: sarrera datuen baliozkotze okerra, bideetara kontrolatu gabeko sarbidea eta fitxategi arriskutsuen murrizpenik gabeko karga.

Konponbidea:

Fabrikatzaileak ondoko partxeak aplikatzea gomendatzen du:

- Patch Roll-up para CPR9 SRx,
- FactoryTalk Linx/Services patch RAID# 1124820,
- FactoryTalk Linx patch RAID# 1126433.

Xehetasuna:

- APIarentzat ikusgai dagoen dei batek erabiltzaileei ahalbidetzen die prozesatzeko fitxategiak ematea sanitizatu gabe. Hori baliatuz erasotzaile batek fitxategi izen bat zehaztu lezake baimendu gabeko kodea exekutatzeko, eta fitxategiak edo datuak aldatzeko. Ahultasun horretarako CVE-2020-11999 identifikatzailea erreserbatu da.
- Fitxategi mota jakin batzuk prozesatzen dituen analisi mekanismoak ez du eskaintzen sarrerako sanititazio prozesurik. Hori baliatuz erasotzaile batek bereziki diseinatutako fitxategiak erabil litzake fitxategien sisteman zehar ibiltzeko, datu konfidentzialak aldatu edo agerian uzteko edo kode arbitrarioa exekutatzeko. Ahultasun horretarako CVE-2020-12001 identifikatzailea erreserbatu da.
- APIarentzat ikusgai dagoen dei batek erabiltzaileei ahalbidetzen die prozesatzeko fitxategiak ematea sanitizatu gabe. Hori baliatuz erasotzaile batek bereziki diseinatutako eskaerak erabil litzake fitxategien sisteman zehar ibiltzeko eta disko gogor lokalean datu konfidentzialak agerian uzteko. Ahultasun horretarako CVE-2020-12003 identifikatzailea erreserbatu da.
- Komunikazio funtzioan dagoen ahultasun batek erabiltzaileei ahalbidetzen die EDS fitxategiak kargatzea FactoryTalk Linx-etik. Hori baliatuz erasotzaile batek konpresio txarreko fitxategi bat karga lezake, eskuragarri dauden CPUaren baliabide guztiak kontsumituz, eta ondorioz zerbitzuaren ukapen egoera sortuko litzateke. Ahultasun horretarako CVE-2020-12005 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Ahultasuna

Ahultasuna Philips-en IntelliBridge Enterprise-n (IBE)

Argitalpen data: 2020/06/12

Garrantzia: Txikia

Kaltetutako baliabideak:

- IntelliBridge Enterprise (IBE), B.12 eta lehenagoko bertsioak.
- Era berean, IntelliBridge Enterprise-ren sistemaren integrazioa ere kaltetuta dago honakoekin egina dagoenean:
  - SureSigns (VS4),
  - EarlyVue (VS30),
  - IntelliVue Guardian (IGS).

Azalpena:

Argitaratu den ahultasuna baliatuz, erasotzaile batek erregistro fitxategietako testu lauan gordetako kredentzialak irakur litzake.

Konponbidea:

- Fabrikatzaileak ahultasun hori konponduko duen bertsio berri bat aurreikusita dauka (IBE B.13) 2020ko laugarren hiruhilekorako.
- Ahultasun honen behin-behineko arintze modura, Philipsek ondokoa gomendatzen du:
  - IBEren transakzioen erregistroak soilik eskura daitezke administratzaile pribilegioekin. IBE sisteman kontu osagarri bat sor daiteke pribilegio mugatuekin, zerbitzu ingeniarientzat.
  - Erregistroen atxikitzea epe onargarri batera murriztea, berreskuratze jarduerak ahalbidetuko dituena.

Xehetasuna:

IntelliBridge Enterprise-n (IBE) jasotzen diren kodifikatu gabeko erabiltzaile kredentzialak transakzioen erregistroetan erregistratzen dira, eta sarbiderako web atari administratiboaren atzean seguru daude. Kaltetutako produktuetatik bidalitako erabiltzaile kredentzial ez zifratuak, Enterprise Systems-ekiko handsake edo autentifikazio ondorioetarako, karga erabilgarri modura erregistratzen dira IntelliBridge Enterprise-n (IBE), transakzioen erregistroen barnean. Pribilegio administratiboak lituzkeen erabiltzaile batek ahultasun hau balia lezake erregistro fitxategietako testu lauan gordetzen diren kredentzialak irakurtzeko. Ahultasun horretarako CVE-2020-12023 identifikatzailea erabili da.

Etiketak: Azpiegitura kritikoak, Ahultasuna

Cross-site Scripting erako ahultasuna OSIsoft-en PI Web API-n

Argitalpen data: 2020/06/12

Garrantzia: Altua

Kaltetutako baliabideak:

PI Web API 2019 Patch 1 (1.12.0.6346) eta lehenagoko bertsio guztiak.

Azalpena:

OSIsoft-ek, OTORIOko Dor Yardeni eta Eliad Mualem-ekin batera, Cross-site Scripting erako ahultasun baten berri eman du. Hori baliatuz erasotzaile batek kode arbitrarioaren urruneko exekuzioa egin lezake.

Konponbidea:

PI Web API 2019 SP1 bertsiora eguneratzea.

Xehetasuna:

OSIsoft-en PI Web APIak duen Cross-site Scripting erako ahultasun bat baliatuz, erasotzaile batek kode arbitrarioaren urruneko exekuzioa egin lezake. Ahultasun horretarako CVE-2020-12021 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Bufferraren gainezkatzea Moxa-ren hainbat produktutan

Argitalpen data: 2020/06/15

Garrantzia: Altua

Kaltetutako baliabideak:

EDR-G902 Series eta EDR-G903 Series routerrak, 5.4 eta lehenagoko bertsioak.

Azalpena:

Claroty-ko Tal Keren-ek pilan (*stack*) oinarritutako bufferraren gainezkatze erako ahultasun baten berri eman du, Moxa-ren hainbat routerri eragiten diena.

Konponbidea:

Firmware-a EDR-G902 Series eta EDR-G903 Series-en 5.5 bertsiora eguneratzea.

Xehetasuna:

Web nabigatzailearen cookiearen asmo gaiztoko funtzionamendua baliatuz, erasotzaile batek pilaren (stack) bufferraren gainezkatzea eragin lezake sistemako web zerbitzarian, bereziki diseinatutako cookie bat erabiliz.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Ahultasuna

Hainbat ahultasun Treck IP protokoloen inplementazioan

Argitalpen data: 2020/06/17

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Kaltetutako produktuak Treck TCP/IP 6.0.1.66 bertsioa baino lehenagokoak dituztenak dira.

Zehazki ondoko protokoloei eragiten die:

- IPv4,
- IPv6,
- UDP,
- DNS,
- DHCP,
- TCP,
- ICMPv4,
- ARP,

Kaltetutako fabrikatzaileetako batzuk honakoak dira:

- B.Braun,
- Caterpillar,
- Green Hills,

- Rockwell,
- Schneider Electric,

Kaltetutako fabrikatzaileen zerrenda osoa Erreferentziak atalean edo esteka honetan kontsulta daiteke.

Azalpena:

JSOF Tech-eko Shlomi Oberman eta Moshe Kol ikertzaileek 'Ripple20' modura ezagutzen diren hainbat ahultasun aurkitu dituzte Treck Inc.-ek garatutako Treck IP protokoloen inplementazioan, hainbat fabrikatzaileren produktuetan jasota dagoena.

Konponbidea:

Treck-ek erabiltzaileei gomendatzen die beren Treck TCP/IP inplementazioaren 6.0.1.66 bertsioa edo goragokoa ezartzea. Informazio gehiago bere webgunean eskura daiteke.

Xehetasuna:

Treck IP protokoloen inplementazioari eragiten dioten 19 ahultasun aurkitu dira guztira. Horietatik 4 kritikoak dira, eta ondorioz hainbat inplementaziotan kodearen urruneko exekuzioa gerta liteke edo memoriaren mugez kanpoko idazketa.

Ahultasunen CVE identifikatzaileak honakoak dira: CVE-2020-11896, CVE-2020-11897, CVE-2020-11898, CVE-2020-11899, CVE-2020-11900, CVE-2020-11901, CVE-2020-11902, CVE-2020-11903, CVE-2020-11904, CVE-2020-11905, CVE-2020-11906, CVE-2020-11907, CVE-2020-11908, CVE-2020-11909, CVE-2020-11910, CVE-2020-11911, CVE-2020-11912, CVE-2020-11913 eta CVE-2020-11914.

Etiketak: Eguneraketa, Azpiegitura kritikoak, IoT, SCADA, Schneider Electric, Ahultasuna

---

Hainbat ahultasun KUKA robotetan

Argitalpen data: 2020/06/18

Garrantzia: Altua

Kaltetutako baliabideak:

KR3R540, KRC4, KSS8.5.7HF1 eta Win7_Embedded sistemak dituzten KUKA robotak.

Azalpena:

Alias Robotics-eko Víctor Mayoral Vilches ikertzaileak larritasun altuko hainbat ahultasun aurkitu ditu KUKA robotek erabilitako sistemetan.

Konponbidea:

Oraingoz ez dago ahultasun horiek konpontzen dituen eguneraketarik.

Gailuetara sarbide fisikoa murriztea gomendatzen da, manipulatuak izan daitezen saihesteko.

Xehetasuna:

Aurkitutako ahultasunak baliatuz, sistemara sarbide fisikoa lukeen erasotzaile batek eragiketarako kritikoak diren zerbitzuak alda litzake Windowsen atazen administratzailetik, eta horrela manipulatzailea gelditu egingo luke.

Gainera, kaltetutako sistemek TRRespass izenaz ezagutzen den ahultasunak eragiten dien DRAM txipak dituzte. Horrek esan nahi du horietan oraindik egin daitezkeela RowHammer erako erasoak.

Ahultasun horiei esleitutako identifikatzaileak CVE-2020-10255 eta CVE-2020-10268 dira.

Etiketak: Ahultasuna

Ahultasuna Johnson Controls-en exacqVision-en

Argitalpen data: 2020/06/19

Garrantzia: Handia

Kaltetutako baliabideak:

- exacqVision Web Service, 20.03.2.0 eta lehenagoko bertsioak;
- exacqVision Enterprise Manager, 20.03.3.0 eta lehenagoko bertsioak.

Azalpena:

exacqVision-ek duen ahultasun bat baliatuz, sinadura kriptografikoaren egiaztapen oker erakoa, administratzaile pribilegioak lituzkeen erasotzaile batek sistema eragilearen komandoak exekuta litzake.

Konponbidea:

- exacqVision Web Service 20.06.2.0 edo ondorengo bertsiora eguneratzea;
- exacqVision Enterprise Manager 20.06.3.0 edo ondorengo bertsiora eguneratzea.

Xehetasuna:

*Software*ak ez du egiaztatzen datuen sinadura kriptografikoa. Hori baliatuz pribilegio administratiboak lituzkeen erasotzaile batek asmo gaiztoko fitxategi bat deskarga eta ireki lezake sistema eragileko komandoak exekutatzeko. Ahultasun horretarako CVE-2020-9047 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Ahultasuna

Hainbat ahultasun Mitsubishi Electric-en produktu batzuetan

Argitalpen data: 2020/06/19

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- MC Works64, 4.02C (10.95.208.31) eta lehenagoko bertsioak;
- MC Works32, 3.00A (9.50.255.02) bertsioa.

Azalpena:

Hainbat ikertzailek 5 ahultasunen berri eman diote ICONICSi, Mitsubishi Electric-en taldeko konpainia. Bat larritasun kritikokoa da eta 4 altuak, mugez kanpoko idazketa, fidagarria ez den informazioaren deserializazio eta kodearen injekzio erakoak.

Konponbidea:

Mitsubishi Electric-ek eskuragarri dagoen software-aren azken bertsiora eguneratzea gomendatzen du.

Xehetasuna:

- Bereziki diseinatutako komunikazio pakete bat kaltetutako produktuetako batera bidaliz gero, zerbitzuaren ukapen egoera (DoS) eragin lezake, edo kodearen urruneko exekuzioa ahalbidetu. Ahultasun horretarako CVE-2020-12011 identifikatzailea erreserbatu da.
- Bereziki diseinatutako komunikazio pakete bat kaltetutako MC Works64 plataformako zerbitzuetara bidaliz gero, zerbitzuaren ukapen egoera (DoS) eragin lezake deserializazio oker baten ondorioz. Ahultasun horretarako CVE-2020-12015 identifikatzailea erreserbatu da.
- Bereziki diseinatutako komunikazio pakete bat kaltetutako MC Works64 produktuaren Workbench Pack & Go funtziora bidaliz gero, kodearen urruneko exekuzioa ahalbidetu lezake deserializazio oker baten ondorioz. Ahultasun horretarako CVE-2020-12009 identifikatzailea erreserbatu da.
- Bereziki diseinatutako mezu bat kaltetutako MC Works64 GridWorX zerbitzariarekin intereaktuatzen duen bezero funtzio pertsonalizatu batetik bidaliz gero, SQL komando arbitrario jakin batzuk exekuta litezke urrunetik, eta barne datuak ezagutzera eman litezke, horrela datu horiek aldatzea ahalbidetuz. Ahultasun horretarako CVE-2020-12013 identifikatzailea erreserbatu da.
- Bereziki diseinatutako komunikazio pakete bat kaltetutako MC Works64 produktuaren FrameWorX zerbitzarira bidaliz gero, kodearen urruneko exekuzioa ahalbidetu lezake urrunetik, eta zerbitzuaren ukapen egoera (DoS) eragin, deserializazio oker baten ondorioz. Ahultasun horretarako CVE-2020-12007 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Ahultasuna

Ahultasunak Iconics Genesis32 eta Genesis64-n

Argitalpen data: 2020/06/19

Garrantzia: Kritikoa

Kaltetutako baliabideak:

GenBroker64, Platform Services, Workbench, FrameWorX Server 10.96 bertsioarekin edo lehenagokoekin erabiltzen duten produktuak honakoak dira:

- GENESIS64,
- Hyper historiador,
- AnalytiX,
- MobileHMI.

GenBroker32 v9.5 bertsioa edo lehenagokoak dituzten produktuak honakoak dira:

- GENESIS32,
- BizViz.

Azalpena:

Claroty, Flashback eta Incite enpresetako eta Oak Ridge Laborategi Nazionaleko ikertzaileek hainbat ahultasun aurkitu dituzte Iconics produktuetan. Horiek baliatuz kodearen urruneko injekzioak edo zerbitzuaren ukapen erako erasoak egin litezke.

Konponbidea:

Ahultasun horiek konpontzeko Iconics-ek 10.96, 10.95.5 eta 10.95.2 bertsioak argitaratuko ditu Genesis64-rako eta 9.4 eta 9.5 bertsioak Genesis32-rako.

Informazio gehiago eskuratzeko Iconics-en webgunera jotzea gomendatzen da.

Xehetasuna:

Iconics-en produktuetan aurkitutako ahultasunak baliatuz mugez kanpoko idazketa erako erasoak, kode injekzioak edo fidagarriak ez diren datuen deserializazioa egin litezke.

Larritasun handieneko ahultasuna izaera kritikokoa da. Hori baliatuz bereziki diseinatutako WCF bezero batek SQL komando arbitrarioak exekuta litezke urrunetik Genesis64 FrameWorX zerbitzarian.

Ahultasun horiei esleitutako identifikatzaileak honakoak dira: CVE-2020-12011, CVE-2020-12015, CVE-2020-12009, CVE-2020-12013 eta CVE-2020-12007.

Etiketak: Eguneraketa, Azpiegitura kritikoak, SCADA, Ahultasuna

---

Hainbat ahultasun BIOTRONIK CardioMessenger II-n

Argitalpen data: 2020/06/19

Garrantzia: Ertaina

Kaltetutako baliabideak:

- CardioMessenger II-S T-Line T4APP 2.20;
- CardioMessenger II-S GSM T4APP 2.20.

Azalpena:

Hainbat ahultasun baliatuz, erasotzaile batek datu konfidentzialak eskura litzake, inplantearen serie zenbakiarekin inplantatutako bihotz gailuetatik transmititutako osasun datuak eskuratu, Cardio Messenger II produktuaren funtzionaltasunari eragin, edo HMU Unitatearen eta APNren arteko komunikazioetan eragin.

Konponbidea:

BIOTRONIKek jakinarazi du ez duela produktuaren segurtasun eguneraketarik argitaratuko, baina, nolanahi ere, kontrol osagarriak ezarri ditu ustiapen arriskua murrizteko eta pazientearen segurtasun arriskuak prebenitzeko. Ahultasun horiek baliatu ahal izatearen arriskua murrizteko, erabiltzaileei gomendatzen die honako neurri babesleak hartzea:

- Etxea monitorizatzeko unitateen kontrol fisiko egokia mantentzea.
- Konfiantzako osasun arretako hornitzaile batengandik edo BIOTRONIKen ordezkari batengatik zuzenean jasotako etxeko monitorizatze unitateak soilik erabiltzea, sistemaren integritatea bermatzearren.
- Produktu hauekin zerikusia duen edozein portaeraren berri osasun arretako zure hornitzaileari edo BIOTRONIKen ordezkari bati ematea.

Xehetasuna:

- Kaltetutako produktuek ez dute ezartzen modu egokian elkarrenganako autentifikazioa BIOTRONIKen urruneko komunikazioaren azpiegiturarekin. Ahultasun horretarako CVE-2019-18246 identifikatzailea erreserbatu da.
- Kaltetutako produktuek kredentzialak testu lauan transmititzen dituzte komunikazio kanal zifratu batera aldatu aurretik. Erasotzaile batek BIOTRONIKen urruneko komunikazioaren azpiegiturara konektatzeko produktuaren bezero kredentzialak ezagutzera eman litzake. Ahultasun horretarako CVE-2019-18248 identifikatzailea erreserbatu da.
- Kaltetutako produktuek kredentzialak berrerabiltzea ahalbidetzen dute hainbat autentifikazio xedetarako. CardioMessenger-era alboko sarbidea lukeen erasotzaile batek BIOTRONIKen urruneko komunikazioaren azpiegiturara konektatzeko erabilitako kredentzialak ezagutzera eman litzake. Ahultasun horretarako CVE-2019-18252 identifikatzailea erreserbatu da.
- Kaltetutako produktuek ez dute informazio konfidentziala zifratzen pausagunean dauden bitartean. CardioMessenger-era sarbide fisikoa lukeen erasotzaile batek osasun neurketen datuak eta CardioMessenger-a parekatuta dagoen inplantatutako bihotz gailuaren serie zenbakia eskura litzake. Ahultasun horretarako CVE-2019-18254 identifikatzailea erreserbatu da.
- Kaltetutako produktuek gailu bakoitzeko kredentzial indibidualak erabiltzen dituzte, berreskura daitekeen formatu batean gordetzen direnak. CardioMessenger-era sarbide fisikoa lukeen erasotzaile batek kredentzial horiek erabil litzake sare autentifikazioa egiteko eta iraganbidean dauden datu lokalak deszifratzeko. Ahultasun horretarako CVE-2019-18256 identifikatzailea erreserbatu da.

Etiketak: Azpiegitura kritikoak, Osasuna, Ahultasuna

Hainbat ahultasun Rockwell Automation FactoryTalk-en

Argitalpen data: 2020/06/19

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Ahultasun hauek FactoryTalk View SE eta FactoryTalk Services Platform-en bertsio guztiei eragiten diete.

Azalpena:

Rockwell Automation-ek, Trend Micro's Zero Day Initiative-rekin lankidetzan, 5 ahultasun argitaratu ditu, bat larritasun kritikokoa, 3 altukoak eta bat ertainekoa. Horiek baliatuz urruneko erasotzaile autentifikatu batek kaltetutako gailuetako datuak manipula litzake, edo urruneko COM objektuak exekutatu pribilegio altuekin.

Konponbidea:

FactoryTalk View SEren kasuan 1126289 eta 1126289 partxeak instalatzea gomendatzen da.Partxe horiek instalatu baino lehen, CPR9 SRx-erako 2020ko apirilaren 6ko 1066644 - Parche Roll-up partxe pilatzailea aplikatu beharra dago.

FactoryTalk View SEren kasuan Rockwell Automation-ek gomendatzen du integratutako segurtasun funtzioak ere gaitzea, bere jakintza baseko 109056 eta 1126943 artikuluetako gida jarraituz IPSec edota HTTP konfiguratzeko.

FactoryTalk Services Platform-en kasuan Rockwell-en jakintza baseko 25612 artikulua erabiltzea gomendatzen da, produktu hau instalatuta dagoen zehazteko. Kasu horretan komunikazio estrategia seguru bat ezarri behar da, jakintza baseko 109056 artikuluan adierazten denaren modukoa.

Xehetasuna:

Rockwell Automation-en produktuetan aurkitutako ahultasunak baliatuz, erasotzaile batek informazio konfidentzialera edo baimendu gabekora sarbidea lor lezake, memoriaren buffer baten mugen barnean baimendu gabeko eragiketak egin, edo sarbide baimenak, kontrolak eta pribilegioak aldatu.

Aurkitutako ahultasunen artetik kritikoena (CVE-2020-12029) gertatzen da fitxategi izenak zuzen ez baliozkotzean proiektuaren direktorio baten barnean. Ondorioz autentifikatu gabeko urruneko erasotzaile batek diseinatutako fitxategi bat exekuta lezake eta kodearen urruneko exekuzioa (RCE) eragin.

Ahultasun horietarako CVE-2020-12029, CVE-2020-12031, CVE-2020-12028, CVE-2020-12027 eta CVE-2020-12033 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Ahultasuna

Sarrera datuen baliozkotze okerra Dräger-en Perseus A500-en

Argitalpen data: 2020/06/19

Garrantzia: Ertaina

Kaltetutako baliabideak:

Dräger Perseus A500, softwarearen 2.00tik 2.02ra bitarteko bertsioak.

Azalpena:

Sarrera datuen baliozkotze desegoki erako ahultasun baten berri eman da Dräger Perseus A500-en.

Konponbidea:

*Softwarea*ren 2.03 bertsiora eguneratzea.

Xehetasuna:

Kaltetutako produktuak ez ditu modu zuzenean baliozkotzen bereziki diseinatutako datu jakin batzuk, Medibus interfazearen bidez doazenak. Horrek eragin lezake kurben ikuspena atzeratzea, eta azken finean berrabiaratze bat gerta liteke berotan. Kontrolatutako aireztapen moduak erabiltzen direnean, berotan egindako abiatze batek aireztapenaren presioa giroan dagoenaren mailaraino jaistea eragiten du, eta horrek pazientearen egoera kaltetu lezake.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Osasuna, Ahultasuna

---

Hainbat ahultasun Baxter-en zenbait produktutan

Argitalpen data: 2020/06/19

Garrantzia: Altua

Kaltetutako baliabideak:

- ExactaMix EM2400, 1.10, 1.11, 1.13 eta 1.14 bertsioak;
- ExactaMix EM1200, 1.1, 1.2, 1.4 eta 1.5 bertsioak;
- PrismaFlex, bertsio guztiak;
- PrisMax, 3.x bertsioaren aurreko guztiak.
- Phoenix Hemodialysis Delivery System SW, 3.36 eta 3.40 bertsioak.

Azalpena:

Baxter-ek 11 ahultasunen berri eman dio CISAri, 6 larritasun altukoak eta 5 ertainekoak, honako era hauetakoak: kredentzialen erabilpena testu lauan, informazio sentikorraren transmisioa testu lauan, informazio sentikorraren zifratze falta, sarbide kontrol desegokia, baliabideen agerpena erabiltzaile desegokiei, sarrera datuen baliozkotze okerra eta autentifikazio desegokia.

Konponbidea:

- ExactaMix EM 2400, 1.10 y 1.11 bertsioen, eta ExactaMix EM1200, 1.1 eta 1.2 bertsioen erabiltzaileek ExactaMix 1.4 (EM1200) eta ExactaMix 1.13 (EM2400) bertsioetara eguneratu behar dute;
- PrismaFlex 8.2x edo bertsio berriagoetara eguneratzea;
- PrisMax eguneratzea DCM (Digital Communication Module) duen PrisMaxv3-ra;
- are gehiago, Baxter-ek erabiltzaile guztiei gomendatzen die dagozkien ohartarazpenetan zehaztutako arintze neurriak ezartzea.

Xehetasuna:

- Kontu administratzailearen kredentzialak testu lauan erabiltzen direla baliatuz, sistemaren baliabideetarako, softwarea exekutatzeko edo fitxategiak, direktorioak edo sistemaren konfigurazioa ikusi/aldatzeko baimendu gabeko sarbidea lukeen erasotzaile batek datu konfidentzialak ikus litzake, PHI barne. Ahultasun horretarako CVE-2020-12016 identifikatzailea erreserbatu da.
- Eskaeren informazioa komunikatzeko formaturik gabeko testu mezuak erabiltzen direla baliatuz, erasotzaile batek sarera sarbidea lortuko luke eta datu konfidentzialak ikusiko lituzke, PHI barne. Ahultasun horretarako CVE-2020-12008 identifikatzailea erreserbatu da.
- Informazio konfidentziala duten gailuko datuak zifratu gabeko dat base batean gordetzen direla baliatuz, sarera sarbidea lukeen erasotzaile batek datu konfidentzialak ikusi edo alda litzake, PHI barne. Ahultasun horretarako CVE-2020-12032 identifikatzailea erreserbatu da.
- SMBv1 atakaren bidezko sarrera datuen baliozkotze okerrak kontrol fluxuari edo sistema baten datuen fluxuari eragin liezaioke. Hori baliatuz urruneko erasotzaile batek informazio konfidentzialera baimendu gabeko sarbidea lortuko luke, zerbitzuaren ukapen egoerak (DoS) sortu edo kode arbitrarioa exekutatu. Ahultasun horretarako CVE-2017-0143 identifikatzailea erabili da.
- Kaltetutako gailuek ez dute autentifikaziorik behar tratamendu datuak PDMS edo EMR sistema batera bidaltzeko konfiguratzen direnean. Hori baliatuz erasotzaile batek tratamenduaren egoeraren informazioa alda lezake. Ahultasun horretarako CVE-2020-12035 identifikatzailea erreserbatu da.
- Sarera sarbidea lukeen erasotzaile batek tratamendu sentikorra ikus lezake, eta baita Phoenix sistemaren eta Exalis tresnaren artean bidalitako preskripzio datuak ere, iraganbidean dauden datuak zifratzeko ezintasunagatik, esate baterako TLS/SSLrekin. Ahultasun horretarako CVE-2020-12048 identifikatzailea erreserbatu da.

Larritasun ertaineko ahultasunetarako honako identifikatzaile hauek erreserbatu dira: CVE-2020-12012, CVE-2020-12024, CVE-2020-12020, CVE-2020-12036 eta CVE-2020-12037.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Osasuna, Ahultasuna

Informazio sentikorra testu lauan transmititze erako ahultasunak Honeywell-en produktuetan

Argitalpen data: 2020/06/25

Garrantzia: Ertaina

Kaltetutako baliabideak:

- ControlEdge PLC, R130.2, R140, R150 eta R151 bertsioak;
- ControlEdge RTU, R101, R110, R140, R150 eta R151 bertsioak.

Azalpena:

Kaspersky-ko Nikolay Sklyarenko-k 2 ahultasunen berri eman dio CISAri, biak larritasun ertainekoak eta informazio sentikorra testu lauan transmititze erakoak.

Konponbidea:

Honeywell-ek informazio zehatza eman du komunikazio ez-segurua Control Edge PLC eta RTU-n arintzeko, SN2020-04-17-01-ConotrolEdge-PLC-and- and-RTU-Secure-Communication dokumentuaren bidez.

Xehetasuna:

- Kaltetutako gailuak zifratu gabeko pasahitzak agerian uzten ditu sarean. Ahultasun horretarako CVE-2020-10628 identifikatzailea erreserbatu da.
- Kaltetutako gailuak saio token bat agerian uzten du sarean. Ahultasun horretarako CVE-2020-10624 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Azpiegitura Kritikoak, Ahultasuna

Ahultasuna Mitsubishi Electric produktuetan

Argitalpen data: 2020/06/25

Garrantzia: Kritikoa

Kaltetutako baliabideak:

CPU moduluen bertsio guztiak MELSEC iQ-R, iQ-F, Q, L eta FX serieetan.

Azalpena:

NESC Lab-eko Shunkai Zhu, Rongkuan Ma eta Peng Cheng-ek ahultasun honen berri eman diote Mitsubishi Electric-i. Hori baliatuz erasotzaile batek komunikazioen datuak atzeman edo manipula litzake, baimendu gabeko eragiketak egin, edo zerbitzuaren ukapen (DoS) erako erasoak burutu.

Konponbidea:

Mitsubishi Electric-ek gomendatzen du komunikazioak zifratzea VPN bat erabiliz, ahultasun honen eragina arintzearren.

Xehetasuna:

Mitsubishi Electric MELSEC-en iQ-R, iQ-F, Q, L eta FX serieetako CPU moduluen eta GX Works3/GX Works2 serieetako CPU moduluen artean testu lauan egindako komunikazioaren ondorioz gertatzen den ahultasun bat baliatuz, erasotzaile batek komunikazioen datuak atzeman edo manipula litzake, baimendu gabeko eragiketak egin, edo zerbitzuaren ukapen (DoS) erako erasoak aurrera eraman. Ahultasun horretarako CVE-2020-14476 identifikatzailea erabili da.

Etiketak: Azpiegitura kritikoak, Ahultasuna

Ahultasunak hainbat robot industrialetan

Argitalpen data: 2020/06/25

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- MiR100, versiones 2.8.1.1 eta lehenagoko bertsioak;
- MiR200;
- MiR250;
- MiR500;
- MiR1000;
- ER200;
- ER-Lite;
- ER-Flex;
- ER-One;
- UVD.

Azalpena:

Alias Robotics-eko hainbat ikertzailek eta Joanneum Research-ek 14 ahultasunen berri eman dute, 7 larritasun kritikokoak, 5 altukoak eta 2 ertainekoak, Mobile Industrial Robots A/S, EasyRobotics, Enabled Robotics eta UVD Robots-en hainbat produkturi eragiten dietenak.

Konponbidea:

Oraingoz ez dago ahultasun horiek konpontzen dituen eguneraketarik.

Xehetasuna:

Erasotzaile batek ohartarazpen honetan azaldutako ahultasunak balia litzake honako ekintzak egiteko:

- kredentzialen erabilpena testu lauan,
- baliabideen agerpena testuinguru desegoki batean,
- funtzio kritikorako autentifikazio falta,
- informazio sentikorraren zifratze falta,
- informazio sentikorraren agerpena baimendu gabeko erabiltzaile bati,
- pasahitzetarako zifratze ahula,
- osokoen bufferraren gainezkatzea,
- sarrera datuen baliozkotze okerra,
- elementu osagabe baten kudeaketan akatsa,
- lehenetsitako baimen okerrak,
- segurtasunean konfiantza informazio gabeziaren bidez,
- sarbidearen kontrol desegokia.

Larritasun kritikoko ahultasunak azaltzen dira jarraian:

- MiR-en (Mobile Industrial Robots) hainbat produkturen kontrol panelera sarbidea lor daiteke IP helbide bat erabiliz testu lauan. Hori baliatuz erasotzaile batek robotaren kontrola har lezake urrunetik, MiR-ek sortu dituen lehenetsitako erabiltzaile interfazeak erabili, autentifikazioa ezabatu eta sare eskaerak zuzenean bidali. Ahultasun horretarako CVE-2020-10270 identifikatzailea erabili da.
- Segurtasun PLCrako pasahitza lehenetsitakoa da. Hori baliatuz manipulatutako programa bat karga liteke PLC horretan, eta horrela objektu bat robotetik gertuegi dagoen kasuetarako larrialdiko geldialdia desgaitu egingo litzateke. Laser eskanerraren konfigurazioa ere kaltetuta gerta liteke. Ahultasun horretarako CVE-2020-10276 identifikatzailea erabili da.
- API RESTerako sarbide tokenak web interfazerako publikoki eskuragarri dauden lehenetsitako kredentzialetatik zuzenean ondorioztatzen dira. Baimendu gabeko erasotzaile batek kredentzial horiek erabil litzake tokena kalkulatzeko, eta API RESTarekin interaktuatzeko datuak iragazi, gehitu edo ezabatuz. Ahultasun horretarako CVE-2020-10275 identifikatzailea erabili da.
- MiR flotako hainbat produktu WiFi MiR (Access Point) moduan aurrekonfiguratuta daude, ondo ezagutzen diren eta oso zabalduta dauden kredentzial batzuekin (SSID eta pasahitza), aspaldiko erabiltzaile gida eta eskuliburuetan jasoak. Ahultasun horretarako CVE-2020-10269 identifikatzailea erabili da.
- MiR-en robot batzuek ROS-en (Robot Operating System) pakete lehenetsiak erabiltzen dituzte, eta konputazio grafikoa inolako autentifikazio motarik gabe erakusten dute. Hori baliatuz haririk gabeko eta kabledun sareetara sarbidea duten erasotzaileek robotaren kontrola har lezakete arazorik gabe. CVE-2020-10269 eta CVE-2020-10271 ahultasunekin batera baliatuz, akats horrek ahalbidetzen du asmo gaiztoko eragileek robota beren nahierara erabiltzea. Ahultasun horretarako CVE-2020-10272 identifikatzailea erabili da.
- MiR-en hainbat robotek ROS-en (Robot Operating System) pakete lehenetsiak erabiltzen dituzte, eta horiek konputazio grafikoa sare interfaze guztien agerian uzten dute, haririk gabekoak nahiz kabledunak izan. CVE-2020-10269 bezalako beste akats batzuekin batera baliatuz, kalkulu grafikoa haririk gabeko sareetatik ere eskura daiteke eta berarekin interaktuatu. Hori baliatuz asmo gaiztoko operadore batek ROSen logikaren kontrola har lezake eta, ondorioz, robot osoarena. Ahultasun horretarako CVE-2020-10271 identifikatzailea erabili da.
- MiR robotaren kontrolatzaileek (konputu unitate zentrala) Ubuntu 16.04.2 erabiltzen dute sistema eragile modura. Horrek segurtasun akatsak ditu, esate baterako erabiltzaileek beren sarbidea eskalatu ahal izatea emana zitzaien mailatik gora fitxategiak sortuz, sarbide lasterketa egoerak, hasierako direktorioaren konfigurazio ez-seguruak eta Zerbitzuaren Ukapen (DoS) erako erasoak ahalbidetzen dituzten balio lehenetsiak. Ahultasun horretarako CVE-2020-10279 identifikatzailea erabili da.

Larritasun altu eta ertaineko ahultasunetarako honako identifikatzaileak erabili dira: CVE-2020-10273, CVE-2020-10274, CVE-2017-18255, CVE-2017-7184, CVE-2020-10280, CVE-2020-10277 eta CVE-2020-10278.

Etiketak: Ahultalsuna

Hainbat ahultasun ENTTEC argi kontrolatzaileetan

Argitalpen data: 2020/06/26

Garrantzia: Handia

Kaltetutako baliabideak:

Ahultasun horiek 70044 firmwarearen 05032019-482 eguneraketari eta lehenagokoei eragiten die, ondoko produktuen kasuan:

- Datagate Mk2,
- Storm 24,
- Pixelator,
- E-Streamer Mk2.

Azalpena:

Argi kontrolatzaileek dituzten hainbat ahultasun argitaratu dira. Horiek baliatuz, erasotzaile batek gailuetara baimendu gabeko SSH/SCP sarbidea lor lezake, asmo gaiztoko kodea injektatu, komandoak exekutatu root pribilegioekin, edo sistemaren direktorioetan fitxategiak irakurri, idatzi edo exekutatu beste edozein erabiltzailek bezala.

Konponbidea:

ENTTECek ez du oraindik inolako eguneraketarik argitaratu. Gailuak firewall-en eta sare kontrol egokien atzean kokatzea gomendatzen du, eta Internetetik sarbiderik ez izatea.

Xehetasuna:

- Root erabiltzaile modura urruneko SSH eta SCP sarbiderako pasahitz barneratuak egotea. Ahultasun horretarako CVE-2019-12776 identifikatzailea erabili da.
- ENTTEC-en Datagate Mk2 web konfigurazioaren softwareak duen gordetako XSS erako hainbat ahultasun baliatuz, autentifikatu gabeko erasotzaile batek asmo gaiztoko kodea injekta lezake aplikazioan zuzenean. Ahultasun horretarako CVE-2019-12774 identifikatzailea erabili da.
- Argi kontrolatzaileek root modura pribilegio altuko sarbidea ahalbidetzen dute sudoren gaitasunaren bidez, sarbide kontrol egoki

bat eskatu gabe. Ahultasun horretarako CVE-2019-12775 identifikatzailea erabili da.
- Sistemak azpiko sistema eragilearen baimenak ordezkatzen ditu, batere seguruak ez diren irakurketa, idazketa eta exekuzio baimenekin erabiltzaile guztientzat. Ahultasun horretarako CVE-2019-12777 identifikatzailea erabili da.

Etiketak: Azpiegitura kritikoak, Ahultasuna

Hainbat ahultasun Rockwell Automation-en zenbait produktutan

Argitalpen data: 2020/06/26

Garrantzia: Handia

Kaltetutako baliabideak:

- FactoryTalk Services Platform, 6.11.00 eta lehenagoko bertsioak;
- FactoryTalk View SE, honako bertsioak:
  - 9.0 eta lehenagokoak;
  - 10.0.

Azalpena:

Applied Risk-ek, ScadaX Security-ko Ilya Karpov eta Evgeny Druzhinin-ekin batera, hiru ahultasunen berri eman dio Rockwell Automation-i, denak larritasun altukoak, XXErako (XML External Entity) erreferentzia desegokiaren murrizpen, informazio sentikorra testu lauan gordetze eta pasahitzaren zifratze ahul erakoak.

Konponbidea:

- 1092746ren argibideak jarraitzea FactoryTalk Services Platform eguneratzeko;
- FactoryTalk View SErekin emandako DeskLock-en bertsio kaltetuen erabiltzaileei gomendatzen zaie softwarearen 10.0 edo ondoreneko bertsio batera eguneratzea.

Xehetasuna:

- Autentifikatu gabeko urruneko erasotzaile batek XML (XXE) kanpo entitate baten erasoa balia lezake gaizki konfiguratutako XML fitxategiak baliatzeko, eta horrela eduki lokalera edo urrunekora sarbidea lortuko luke. Honek zerbitzuaren ukapen egoera (DoS) eragin lezake, eta erasotzaileak edozein fitxategi lokal irakur lezake arbitrarioki, sistemaren mailako zerbitzuen bidez. Ahultasun horretarako CVE-2020-14478 identifikatzailea erreserbatu da.
- Kredentzialak RAMean gordetzen direnez formaturik gabe, erasotzaile lokal autentifikatu batek sarbidea lor lezake kredentzial batzuetara, Windowseko saio hasierakoetara barne. Ahultasun horretarako CVE-2020-14480 identifikatzailea erreserbatu da.
- FactoryTalk View SErekin emandako DeskLock tresnak zifratze algoritmo ahul bat erabiltzen du. Hori baliatuz autentifikatutako erasotzaile lokal batek erabiltzaile kredentzialak deszifra litzake, Windowseko erabiltzailea edo Windows DeskLock-eko pasahitzak barne. Arriskuan dagoen erabiltzaile batek kontu administratibo bat baldin badauka, erasotzaileak sarbide osoa lor lezake erabiltzailearen sistema eragilera eta FactoryTalk View SEren osagai batzuetara. Ahultasun horretarako CVE-2020-14481 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Azpiegitura Kritikoak, Ahultasuna

Autentifikazio akatsak Philips Ultrasound Systems-en

Argitalpen data: 2020/06/26

Garrantzia: Txikia

Kaltetutako baliabideak:

- Ultrasonido ClearVue, 3.2 eta lehenagoko bertsioak.
- Ultrasonido CX, 5.0.2 eta lehenagoko bertsioak.
- Ultrasonido EPIQ / Affiniti, VM5.0 eta lehenagoko bertsioak.
- Ultrasonido Sparq, 3.0.2 eta lehenagoko bertsioak.
- Ultrasonido Xperius, bertsio guztiak.

Azalpena:

Philipsek informatu duenaren arabera, bere Ultrasound Systems produktuek duten ahultasuna baliatuz, autentifikatu gabeko erasotzaile batek sistemako informazioa ikusi edo alda lezake.

Konponbidea:

Ultrasound EPIQ / Affiniti-ren 2020ko apirileko bertsioa instalatzea gomendatzen da, VM6.0 bertsioa.Bestalde, Philipsek Ultrasound EPIQ / Affiniti sistemen erabiltzaileei gomendatzen die beren eskualdeko zerbitzuarekin harremanetan jartzea.

Beste produktu batzuen kasuan ahultasuna ondorengo bertsioetan konpontzea aurreikusten da:

- Ultrasound ClearVue 3.3 bertsioa, 2020ko laugarren hiruhilekorako aurreikusia.
- Ultrasound CX5.0.3 bertsioa, 2020ko laugarren hiruhilekorako aurreikusia.
- Ultrasound Sparq 3.0.3 bertsioa, 2020ko laugarren hiruhilekorako aurreikusia.

Bestalde, Philipsek gomendatzen du gailuak erabiltzen dituzten zerbitzu hornitzaileek gailuen eskuragarritasuna izan dezaten bermatzea. zerbitzuaren eragiketa lanek irauten duten bitartean.

Philipsen zerbitzu teknikoarekin edo bakoitzaren eskualdeko zerbitzuarekin harremanetan jartzea gomendatzen da.

Xehetasuna:

Philips Ultrasound Systems produktuetan antzemandako ahultasuna baliatuz erasotzaile batek saioaren hasierako autentifikaziorik behar ez duen bide edo kanal alternatibo bat erabil lezake informazioa ikusi edo aldatzeko. Ahultasun horretarako CVE-2020-14477 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Osasuna, Ahultasuna