2019ko Urriaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Bufferraren gainezkatzea Moxa-ren EDR-810 serieko routerretan

Argitalpen data: 2019/10/02

Garrantzia: Altua

Kaltetutako baliabideak:

EDR-810 serieko routerrak, *firmware*-aren 5.1 eta lehenagoko bertsioak.

Azalpena:

Moxak pilan (*stack*) oinarritutako bufferraren gainezkatze erako ahultasun baten berri eman du, EDR-810 serieko routerrei eragiten diena.Ahultasun hori arrakastaz baliatuz gero, erasotzaile batek kode arbitrarioa exekuta lezake.

Konponbidea:

Moxak ahultasun hori konpontzen duen *firmware*-aren eguneraketa bat argitaratu du.

Xehetasuna:

Web zerbitzariaren hainbat funtzio baliatuz, erasotzaile batek bufferraren gainezkatzea eragin lezake, eta horrela kode arbitrarioa exekutatzea lortu.

Etiketak: Eguneraketa, Ahultasuna

CSRF erako ahultasuna SMA Solar Technology AGren Sunny WebBox-en

Argitalpen data: 2019/10/09

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Sunny WebBox, *firmware*-aren 1.6 eta lehenagoko bertsioak.

Azalpena:

Leongo Unibertsitateko Borja Merino eta Eduardo Villaverde ikertzaileek, INCIBEko Sistemas de Control Industrial-eko zibersegurtasun arloko Carlos del Canto eta Victor Fidalgo-rekin batera, CSRF (*Cross-Site Request Forgery*) erako ahultasun baten berri eman dute. Hori baliatuz urruneko erasotzaile batek ekintzak egin litzake erabiltzailearen baimenekin.

Konponbidea:

Oraingo produktuak ez dauka zerbitzurik, eta horregatik SMAk ondoko neurriak hartzea gomendatzen du:

- Ataken birbideratzea desgaitzea eta VPN bat erabiltzea.
- Lehenetsitako pasahitz guztiak aldatzea.
- Erabili behar ez diren sistemako edo router-eko ataka guztiak ixtea.

Xehetasuna:

Erasotzaile batek ahultasun hau baliatuko balu, ondokoa egin lezake: zerbitzuaren ukapen egoera eragin, pasahitzak aldatu, zerbitzuak aktibatu, *man-in-the-middle* erasoak egin eta gailuen sarrera parametroak aldatu, adibidez sentsoreak. Erasotzaileak asmo gaiztoko

esteka bat bidaliko balio autentifikatutako operadore bati, honek ekintzak egin ahal izango lituzke erabiltzaile horren baimenekin. Ahultasun horretarako CVE-2019-13529 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun GEren Mark Vle kontrolatzailean

Argitalpen data: 2019/10/09

Garrantzia: Ertaina

Kaltetutako baliabideak:

Mark Vle kontrolatzailearen bertsio guztiak.

Azalpena:

Claroty-ko Sharon Brizinov ikertzaileak Mark Vle kontrolatzaileari eragiten dion softwareak dituen hainbat ahultasunen berri eman du. Ahultasun hori arrakastaz baliatuz gero, erasotzaile batek gailua irakur lezake, bertan idatzi edo komandoak exekutatu.

Konponbidea:

Arazo horiek arintzeko GEk ondoko konponbideak gomendatzen ditu:

- Telnet zerbitzua desgaitzea, Mark Vle kontrolatzailearen 6.0 eta lehenagoko bertsioetan gaiturik dagoena modu lehenetsian.
- Mark Vle kontrolatzailea ingurune operatiboaren barnean hedatzean pasahitza aldatzea.

Xehetasuna:

- Ahultasun baten jatorria da Telnet protokoloaren inplementazio ez seguru bat gailuan. Erasotzaile batek autentifikatzea lor lezake lehenetsitako kredentzialekin. Ahultasun horretarako CVE-2019-13554 identifikatzailea erreserbatu da.
- Beste ahultasunaren jatorria da gailuan barneratutako kredentzialak egotea *root* pribilegioekin. Erasotzaile batek kontrolatzailera sartzea lor lezake *root* pribilegioekin.

Etiketak: Eguneraketa, Ahultasuna

Zerbitzuaren ukapena Beckhoff Automation-en TwinCAT Profinet driverren

Argitalpen data: 2019/10/10

Garrantzia: Altua

Kaltetutako baliabideak:

Ondoko bertsio hauen berdinak edo lehenagokoak:

- TwinCAT 2 Build 2304,
- TwinCAT 3.1 Build 4024.0.

Azalpena:

Rapid7-ko Andreas Galauner ikertzaileak hainbat gailuri eragiten dien kritikotasun altuko ahultasun baten berri eman du. Urruneko erasotzaile batek zerbitzuaren ukapen egoera eragin lezake gailuetan.

Konponbidea:

Ahultasuna konpontzen duen eguneraketarik oraindik ez dago, baina Bechoff-ek lan horretan dihardu. Bitartean firewall-ean arauak ezartzea gomendatzen dute, fidagarriak ez diren sareetatik gailura datozen PROFINET DCP paketeak blokeatzeko.

Xehetasuna:

TwinCAT-ek Profinet kontrolatzaile bat dauka garapen ingurune batean konfiguratu litekeena Profinet konexioak kontrolatzailera bidaltzeko. Hori konfiguratu baldin bada, manipulatutako Profinet DCP paketeak bidal litezke. Urruneko erasotzaile batek manipulatutako pakete horiek bidal litzake gailuetan zerbitzuaren ukapen egoera eragiteko. Ahultasun horretarako CVE-2019-5637 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna

Hainbat ahultasun Dräger-en Infinity M300 produktuetan

Argitalpen data: 2019/10/11

Garrantzia: Altua

Kaltetutako baliabideak:

Infinity® M300, VG2.3.1 eta lehenagoko bertsioak.

Azalpena:

Dräger-ek zerbitzuaren ukapen eta informazioaren agerpen erako hainbat ahultasun aurkitu ditu. Horiek baliatuz urruneko erasotzaile batek gailuan zerbitzuaren ukapen egoera eragin lezake, eta ospitaleko sarearen bitartez zabaldutako informazioa eskuratu.

Konponbidea:

Drägerrek 2020ko martxoan softwarearen eguneraketa bat argitaratuko du, VG2.3.2 bertsioa.

Xehetasuna:

- Baimenik gabeko erasotzaile batek ospitaleko sarean zerbitzuaren ukapen erako eraso bat egingo balu, Infinity sarea arriskuan jar liteke eta Infinity M300 produktuak berrabiaraz litezke, edo haiek beren haririk gabeko komunikazioa gal lezakete. Berrabiarazte batek 30 segundo irauten ditu gutxi gorabehera, eta denbora horretan gaixoaren monitorizazioa galdu egingo litzateke; nolanahi ere, modu automatikoan berreskuratuko litzateke. Infinity CentralStation-ek soinuz eta argiz abisatuko luke Infinity M300 deskonektaturik dagoela.
- Zerbitzuaren ukapen erako eraso errepikakor batek Infinity M300 errore egoeran gelditzea eragin lezake, eta ondorioz eskuz berrabiatu beharko litzateke.
- Baimenik gabeko erasotzaile batek ospitaleko sarera sartzea eta Infinity sarea erasotzea lortuko balu, Infinity CentralStation eta Infinity M300en artean bidalitako informazioa arriskuan egongo litzateke, eta erasotzaileak alarmen ezarpenak aldatu ahal izango lituzke, haiek itzali edo M300 gailua etenaldi edo deskarga egoeran jarri.

Etiketak: Ahultasuna

Bufferraren gainezkatze erako ahultasuna AVEVAren IEC870IP driverrean

Argitalpen data: 2019/10/15

Garrantzia: Altua

Kaltetutako baliabideak:

Vijeo Citect eta Citect SCADArako IEC870IP driverra, 4.14.02 eta lehenagoko bertsioak.

Azalpena:

IIT Kanpur zentroko VAPT ekipoak, ICS-CERTekin lankidetzan, memoriaren gainezkatze erako ahultasun bat aurkitu du. Hori baliatuz erasotzaile batek zerbitzaria erortzea eragin lezake eta funtzionamenduz kanpo utzi.

Konponbidea:

Kaltetutako produktuak 4.15.00 bertsiora eguneratzea gomendatzen da.

Xehetasuna:

IEC870IP driverraren bertsio ahulei bufferraren gainezkatzeak eragin egiten die. Erasotzaile batek ahultasun hori baliatuz gero zerbitzariak ondo funtzionatzeari uztea eragin lezake.

Etiketak: Eguneraketa, SCADA, Ahultasuna

Hainbat ahultasun Phoenix Contact-en Automation Worx Software Suite-n

Argitalpen data: 2019/10/15

Garrantzia: Altua

Kaltetutako baliabideak:

- PC Worx, 1.86 eta lehenagoko bertsioak.
- PC Worx Express, 1.86 eta lehenagoko bertsioak.
- Config, 1.86 eta lehenagoko bertsioak.

Azalpena:

NCCIC eta koordinaturik, 9sg Security Team-eko ekipoak hainbat eratako ahultasunen berri eman du, mugez kanpoko irakurketa eta memoriaren hondatze erakoak, urruneko kodearen exekuzioaren ondorioz sortuak, sarrera datuen baliozkotze oker batek eraginda.

Konponbidea:

Produktuaren hurrengo bertsioan arazo horiek konpontzeko hobekuntzak egingo dira. Bitartean, ahultasun horiek arintzeko neurri batzuk aplikatzea gomendatzen da:

- Proiektuen fitxategiak partekatzean, transferentziarako zerbitzu seguruak erabiltzea.
- Emailen bidez informazio sentikorra ez partekatzea zifratuta ez badago.

Xehetasuna:

PC Works edo Config proiektuetako aldaketak baliatuz, erasotzaile batek urruneko kodea exekuta lezake, sarrerako datuen baliozkotze oker baten ondorioz. Erasotzaileak Worx edo Config proiektuekin gailurako sarbidea eduki beharra dauka proiektuko datuak eta fitxategiak aldatu ahal izateko. Erasotzaileak jatorrizko fitxategiak aldatutako fitxategiekin ordezten ditu, eta horrela eragiten du erasoa. Ahultasun horretarako CVE-2019-16675 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Ahultasuna Eaton-en hainbat produktutan

Argitalpen data: 2019/10/18

Garrantzia: Altua

Kaltetutako baliabideak:

- CGLine Web Controller, Z1000.H eta lehenagoko bertsioak,
- CGVision, 6.02 bertsiotik 6.40 bertsiora bitartekoak.

Azalpena:

Eaton-ek CGLine Web Controller-i eragiten dion ahultasun baten berri eman du, CGVision gainbegiratze softwarera konektatzen denean.

Konponbidea:

- CGLine Web Controller, Z1000.J bertsiora eguneratzea. Firmwarearen bertsio berria deskargatu ahal izateko, Eaton-en arreta zerbitzuarekin harremanetan jarri beharra dago.
- CGVision-en kasuan eguneraketa bat aurreikusita dago 2019ko azarorako.

Xehetasuna:

CGVision gainbegiratze softwarea CGLine Web Controller gailura konektatzean, bi gailuei eragiten dien ahultasun bat sortzen da. CGVision-era konektatuta ez dauden edo horrek gainbegiratzen ez dituen CGLine Web Controller gailuak ez ditu eragiten ahultasun honek.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Horner Automation-en Cscape-n

Argitalpen data: 2019/10/18

Garrantzia: Altua

Kaltetutako baliabideak:

Cscape, 9.90 bertsioa eta lehenagokoak.

Azalpena:

Protek Research Lab-eko Francis Provencher ikertzaileak, Trend Microko Zero Day Initiative-rekin batera, mugez kanpoko idazketa erako eta sarreren baliozkotze desegoki erako ahultasunen berri eman du. Horiek baliatuz informaziora sarbidea lor liteke eta kodea modu arbitrarioan exekutatu.

Konponbidea:

Horner Automation-ek kaltetutako erabiltzaileei gomendatzen die Cscape-ren 9.90 SP1 edo goragoko bertsioetara eguneratzea, Ameriketako Estatu Batuetarako edo munduko gainerako herrialdeetarako eskuragarri daudenak.

Xehetasuna:

- Fitxategien prozesamenduak duen baliozkotze oker bat baliatuz, erasotzaile batek bereziki diseinatutako fitxategiak sor litzake. Horrela informazio konfidentzialera sarbidea lor lezake edo kode arbitrarioa urrunetik exekutatu. Ahultasun horretarako CVE-2019-13541 identifikatzailea erreserbatu da.
- Datuen baliozkotze oker batek eraginda, sistemak bufferraren aurreikusitako zonatik kanpo idaztea gerta liteke, eta horren ondorioz erasotzaile batek kodea arbitrarioki exekuta lezake. Ahultasun horretarako CVE-2019-13545 identifikatzailea erreserbatu da

Etiketak: Eguneraketa, Ahultasuna

Autentifikazio okerra ABBren hainbat gailutan

Argitalpen data: 2019/10/18

Garrantzia: Txikia

Kaltetutako baliabideak:

- UNO-DM, 1.8.2 bertsioa eta lehenagokoak;
- PVS-100-TL eta PVS120-TL, 0.10.14 bertsioa eta lehenagokoak;
- PVS-175-TL, 0.2.6 bertsioa eta lehenagokoak;
- PVS-50/60 eta TRIO-TM, 1.2.15 bertsioa eta lehenagokoak;
- REACT 2, 0.2.19 bertsioa eta lehenagokoak.

Azalpena:

Maxim Rupp ikertzaileak autentifikazio oker erako ahultasun baten berri eman du. Hori baliatuz erasotzaile batek kaltetutako produktuen informaziora sarbidea lor lezake autentifikatu behar izan gabe.

Konponbidea:

Honako bertsio hauetara eguneratzea:

- **UNO-DM, 1.8.3 bertsioa.**

- **PVS-100-TL eta PVS120-TL, 0.10.15 bertsioa.**
- **PVS-175-TL, 0.2.7 bertsioa.**
- **PVS-50/60 eta TRIO-TM, 1.2.16 bertsioa.**
- **REACT 2, 0.2.20 bertsioa.**

Xehetasuna:

Autentifikazio oker erako ahultasuna baliatuz, produktuak zenbait informaziora irakurketa moduan sarbidea izatea lor liteke, aldez aurretik autentifikazio prozesu bat egin behar izan gabe. Ahultasun horretarako ez da identifikatzailerik esleitu

Etiketak: Eguneraketa, Ahultasuna

Bufferraren gainezkatze erako ahultasuna 3S-Smart Software Solutions GmbH-ren CODESYS ENI-n

Argitalpen data: 2019/10/24

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- CODESYS V2.3 ENI zerbitzariak, 3.2.2.25 baino lehenagoko bertsioak.
- CODESYS V2.3 konfigurazioak, 2.3.9.61 baino lehenagoko bertsioak, kaltetutako CODESYS ENI zerbitzariaren bertsio ahulak baitituzte.

Azalpena:

Bufferraren gainezkatze erako ahultasun bat aurkitu da, 3S-Smart Software Solutions GmbH-ren ENI zerbitzariei eragiten diena. Erasotzaile batek urrunetik zerbitzuaren ukapen egoera eragitea edo kode arbitrarioa exekutatzea lor lezake.

Konponbidea:

Ahultasun hau konpontzeko fabrikatzaileak kaltetutako produktua 3.2.2.25 bertsiora eguneratzea gomendatzen du.

Xehetasuna:

Urruneko erasotzaile batek pilan (stack) oinarritutako bufferraren gainezkatze erako ahultasuna balia lezake, zerbitzuaren ukapen egoera eragiteko edo kode arbitrarioa exekutatzeko. Ahultasun horretarako CVE-2019-16265 identifikatzailea erreserbatu da

Etiketak: Eguneraketa, Ahultasuna

Autentifikaziorik eza Honeywell-en IP-AK2-n

Argitalpen data: 2019/10/25

Garrantzia: Ertaina

Kaltetutako baliabideak:

- IP-AK2 sarbide kontrolaren panela, 1.04.07 bertsioa eta lehenagokoak.

Azalpena:

Maxim Rupp ikertzaileak funtzio kritikoan autentifikaziorik eza erako ahultasun baten berri eman du. Hori baliatuz erasotzaile batek konfigurazio fitxategiak deskarga litzake autentifikaziorik gabeko URL baten bidez, konfigurazioa eta baimendutako bisitarien informazioa agerian utziz.

Konponbidea:

1.04.15 bertsiora eguneratzea.

Xehetasuna:

Kaltetutako gailuetan barneratutako web zerbitzaria baliatuz, autentifikaziorik gabeko urruneko erasotzaileek webaren konfigurazio datuak eskura litzakete. Ahultasun horretarako CVE-2019-13525 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Rittal-en Chiller SK 3232-Series-en

Argitalpen data: 2019/10/25

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Chiller SK 3232-Series-en web interfazea, Carel pCOWeb A1.5.3 - B1.2.4 *firmware*-an oinarritua.

Azalpena:

Applied Risk-ek funtzio kritikoan autentifikaziorik eza erako eta kredentzial barneratuen erabilpen erako hainbat ahultasunen berri eman du, Rittal-en Chiller SK 3232-Series produktuak dituenak. Ahultasun horiek arrakastaz baliatuz gero, kaltetutako osagaiaren lehen mailako eragiketak eten egin litezke, beste ekipo batzuen hoztea itzali eta tenperatura doitzeko puntuan aldaketak ahalbidetu.

Konponbidea:

Ahultasun hauen arintzeei buruzko informazioa eskuratzeko, Rittal-en zerbitzuarekin harremanetan jartzea gomendatzen da honako helbide elektronikoan:

Xehetasuna:

- Kaltetutako sistemetako autentifikazio mekanismoak ez du babes maila nahikorik eskaintzen baimendu gabeko konfigurazio aldaketen aurrean. Lehen mailako eragiketak, hau da, hozte unitatea piztea eta itzaltzea eta tenperaturaren doitze puntuaren doitzea, autentifikatu behar izan gabe alda daitezke. Ahultasun horretarako CVE-2019-13549 identifikatzailea erreserbatu da.
- Kaltetutako sistemetan barneratutako kredentzialak erabiliz konfiguratzen da autentifikazio mekanismoa. Kredentzial horiek baliatuz erasotzaileek lehen mailako eragiketetan eragin lezakete, hau da, hozte unitatea piztu eta itzali, eta tenperaturaren doitze puntua ezarri. Ahultasun horretarako CVE-2019-13553 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Ahultasuna

Baliabideen agerpena Philips-en IntelliSpace Perinatal-en

Argitalpen data: 2019/10/25

Garrantzia: Ertaina

Kaltetutako baliabideak:

IntelliSpace Perinatal, K bertsioa eta lehenagokoak.

Azalpena:

Philipsek kritikotasun ertaineko ahultasun bat aurkitu du. Erasotzaile batek sistemako baliabideetara baimenik gabeko sarbidea lor lezake, softwarearen exekuzioa barne, edo fitxategiak, direktorioak edo sistemaren konfigurazioa ikusi/aldatu.

Konponbidea:

Philips-ek Philips InCenter atarian eskuragarri dagoen dokumentazioa eguneratuko du, arintzeei buruzko gida argi bat eskaintzeko.

Xehetasuna:

IntelliSpace Perinatal aplikazioaren ingurunearen barneko ahultasun bat baliatuz, blokeatutako aplikazio baten pantailara sarbide fisikoa lukeen baimenik gabeko erasotzaile batek, edo urruneko mahai-gaineko saioaren aplikazioaren erabiltzaile baimendu batek Windows sistema eragilearen baimendu gabeko baliabideetara sarbidea lor lezakete, sarbide mugatuko Windows erabiltzaile modura. Windowsen balizko ahultasunak direla eta, litekeena da eraso modu osagarriak erabiltzea sistema eragilean pribilegioak eskalatzeko. Ahultasun horretarako CVE-2019-13546 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun ABBren produktuetan

Argitalpen data: 2019/10/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Relion 650 series, 2.1.0.2 bertsioa eta lehenagokoak;
- Relion 670 series, 2.1.0.2 bertsioa eta lehenagokoak;
- Relion 670 series, 1p1r26 bertsioa eta lehenagokoak.

Azalpena:

Hainbat eratako ahultasunak argitaratu dira: zerbitzuaren ukapena, informazioaren agerpena eta fitxategietara baimenik gabeko sarbidea. Horiek baliatuz erasotzaile batek informazio sentikorra eskura lezake edo zerbitzuaren ukapen egoera eragin.

Konponbidea:

Kaltetutako produktuak azken bertsiora eguneratzea. Informazio gehiago eskuratzeko erreferentzien atala irakurri.

Xehetasuna:

Erasotzaile batek ohartarazpen honetan azaldutako ahultasunen bat balia lezake honako ekintza hauetakoren bat egin ahal izateko:

- zerbitzuaren ukapena,
- informazioaren zabalkundea,
- flash unitateko edozein fitxategi berreskuratu.

Honako identifikatzaile hauek esleitu dira: CVE-2016-2109, CVE-2016-2177, CVE-2016-2178, CVE-2016-2182, CVE-2016-2183, CVE-2016-6304, CVE-2016-6306, CVE-2017-3737, CVE-2018-0739, CVE-2018-0737 eta CVE-2018-0732.

Etiketak: Eguneraketa, Ahultasuna

Alboko sareetara baimenik gabeko sarbidea Phoenix Contact-en FL NAT produktuetan

Argitalpen data: 2019/10/28

Garrantzia: Altua

Kaltetutako baliabideak:

- FL NAT 2208;
- FL NAT 2304-2GC-2SFP.

Azalpena:

Phoenix Contact-ek kritikotasun altuko ahultasun bat aurkitu du FL NAT gailuetan. Erasotzaile batek gailuaren alboko azpi-sareetara baimenik gabeko sarbidea lor lezake.

Konponbidea:

Ahultasun horretarako Phoenix Contact-ek firmwarearen eguneraketa bat argitaratuko du (V2.90) 2020ko bigarren hiruhilekoan.

Xehetasuna:

Ahultasuna gerta daiteke MAC o 802.1x atakan oinarritutako segurtasunak gaituta baldin badaude. Kaltetutako gailuek alboko azpi-sareetara baimenik gabeko sarbidea ahalbidetu lezakete, transmisio bideratu bat egiten bada. Erasotzaile batek gailuaren alboko azpi-sareetara baimenik gabeko sarbidea lor lezake. Ahultasun horretarako CVE-2019-18352 identifikatzailea erreserbatu da

Etiketak: Ahultasuna