2019ko Uztailaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Sarreraren baliozkotze okerra Quest-en KACE Systems Management Appliance-n (SMA)nce (SMA) de Quest

Argitalpen data: 2019/07/03

Garrantzia: Txikia

Kaltetutako baliabideak:

- KACE SMA, 8.0.x bertsio guztiak;
- KACE SMA, 8.1.x bertsio guztiak;
- KACE SMA, 9.0.x bertsio guztiak.

Azalpena:

Juan Pablo Lopez Yacubian ikertzaileak sarreraren baliozkotze oker erako ahultasun bat aurkitu du. Ahultasun hori arrakastaz baliatuz gero erabiltzaile administratzaile bat nahi gabe sar liteke gailuaren azpiko sistema eragilean.

Konponbidea:

Quest-ek kaltetutako erabiltzaileei gomendatzen die 9.1 bertsiora edo berriagora eguneratzea.

Xehetasuna:

Ahultasun honek gailura nahi gabe sartzea ahalbidetzen du, administratzailearen erabiltzaile interfazean kokatuta dauden arazoak konpontzeko tresnen funtzioak baliatuz. Ahultasun horretarako CVE-2019-10973 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Siemens produktuetan

Argitalpen data: 2019/07/09

Garrantzia: Handia

Kaltetutako baliabideak:

- SIMATIC PCS 7 V8.0 eta lehenagoko bertsioak,
- SIMATIC PCS 7 V8.1, bertsio guztiak,
- SIMATIC PCS 7, WinCC V7.4 SP1 Upd11 duten V8.2 SP1 baino lehenagoko bertsio guztiak,
- SIMATIC PCS 7, WinCC V7.4 SP1 Upd11 duten V9.0 SP2 baino lehenagoko bertsio guztiak,
- SIMATIC WinCC Professional V13, V14 eta V15, bertsio guztiak,
- SIMATIC WinCC Runtime Professional V13, V14 eta V5, bertsio guztiak,
- SIMATIC WinCC V7.2 eta lehenagoko bertsioak,
- SIMATIC WinCC V7.3, bertsio guztiak,
- SIMATIC WinCC, V7.4 SP1 Upd 11 bertsioa baino lehenagoko guztiak,
- SIMATIC WinCC, V7-5 Upd 3 bertsioa baino lehenagoko guztiak,
- SIMATIC RF615R, V3.2.1 bertsioa baino lehenagoko guztiak,
- SIMATIC RF68XR, V3.2.1 bertsioa baino lehenagoko guztiak,
- SIMATIC Field PG M4, M5 eta M6, bertsio guztiak,
- SIMATIC IPC127E, IPC2X7E, IPC3000 SMART V2, IPC327E, IPC347E, IPC377E, IPC427C, IPC427D, IPC427D, IPC477C, IPC477D, IPC527G, IPC547E, IPC547E, IPC547G, IPC627C, IPC627D, IPC647C, IPC647D, IPC677C, IPC677D, IPC827C, IPC827D, IPC847C, IPC847D eta ITP1000, bertsio guztiak,
- SIMATIC IPC427E, BIOSaren V21.01.11 bertsioa baino lehenagoko guztiak,

- SIMATIC IPC477E, BIOSaren V21.01.11 bertsioa baino lehenagoko guztiak,
- SIMATIC IPC627E, BIOSaren V25.02.04 bertsioa baino lehenagoko guztiak,
- SIMATIC IPC647E, BIOSaren V25.02.04 bertsioa baino lehenagoko guztiak,
- SIMATIC IPC677E, BIOSaren V25.02.04 bertsioa baino lehenagoko guztiak,
- SIMATIC IPC847E, BIOSaren V25.02.04 bertsioa baino lehenagoko guztiak,
- SIMATIC S7-1500 CPU S7-1518-4 PN/DP MFP (MLFB: 6ES7518-4AX00-1AC0), bertsio guztiak,
- SIMATIC S7-1500 CPU S7-1518F-4 PN/DP MFP (MLFB: 6ES7518-4FX00-1AC0), bertsio guztiak,
- SIMOTION P320-4E, bertsio guztiak,
- SIMOTION P320-4S, bertsio guztiak,
- SINUMERIK 840 D sl (NCU720.3B, NCU730.3B, NCU720.3, NCU730.3), bertsio guztiak,
- SINUMERIK PCU 50.5, bertsio guztiak,
- SINUMERIK Panels with integrated TCU, bertsio guztiak,
- SINUMERIK TCU 30.3, bertsio guztiak,
- TIA Administrator, V1.0 SP1 Upd1 baino lehenagoko bertsio guztiak,
- Spectrum Power 3 (Corporate User Interface) V3.11 eta lehenagokoak,
- Spectrum Power 4 (Corporate User Interface) V4.75,
- Spectrum Power 5 (Corporate User Interface) V5.50 eta lehenagokoak,
- Spectrum Power 7 (Corporate User Interface) V2.20 eta lehenagokoak,
- SIPROTEC 5, ondoko gailu motekin: 6MD85, 6MD86,6MD89, 7UM85, 7SA87, 7SD87, 7SL87, 7VK87,7SA82, 7SA86, 7SD82, 7SD86, 7SL82, 7SL86,7SJ86, 7SK82, 7SK85, 7SJ82, 7SJ85, 7UT82,7UT85, 7UT86, 7UT87 eta 7VE85; CPU ezberdinekin (CP300 eta CP100), eta dagozkien Ethernet komunikazio moduluak, V7.90 bertsioa baino lehenagoko guztiak.
- Beste SIPROTEC 5 batzuk, CPU mota ezberdinekin (CP300 eta CP100) eta dagozkien Ethernet komunikazio moduluak, bertsio guztiak,
- SIPROTEC 5 erreleak, CPU ezberdinekin (CP200) eta dagozkien Ethernet komunikazio moduluak, bertsio guztiak,
- DIGSI 5 engineering software, V7.90 bertsioa baino lehenagoko guztiak.

Azalpena:

Hainbat eratako ahultasunak argitaratu dira: sistemara fitxategiak kargatzean kontrol falta, web komunikazioetan zifratze sendoaren falta, autentifikatutako erabiltzaile batek mikroarkitekturaren sekzioetara izan beharko ez lukeen sarbidea, web aplikazioan autentifikazioari ihesa, Cross-Site Scripting (XSS) eta neurrira egindako paketeen bidalketa. Ahultasun horiek baliatuz gero, erasotzaile batek kode arbitrarioa exekuta lezake, informazio sentikorra eskuratu, web aplikazioan komandoak exekutatu eta sisteman fitxategiak aldatu, igo edo ezabatu.

Konponbidea:

Siemensek hainbat eguneraketa garatu ditu kaltetutako gailuentzat.

Xehetasuna:

Ondoren zehazten dira larritasun altuko ahultasunak:

- Konfigurazio integratua duen web aplikazioak (TIA Administrator) erasotzaile bati ahalbidetuko lioke aplikazioko zenbait komando exekutatzea beharrezko autentifikaziorik gabe. Ahultasun horretarako CVE-2019-10915 identifikatzailea erabili da..
- Urruneko erasotzaile batek bereziki diseinatutako paketeak bidal litzake TCP 443 atakatik sistemako fitxategien barnean fitxategiak kargatu edo deskargatzeko. Ahultasun horretarako CVE-2019-10930 identifikatzailea erabili da.
- Urruneko erasotzaile batek bereziki diseinatutako paketeak bidal litzake TCP 443 atakatik, eta horrela zerbitzuaren ukapen egoera (DoS) eragin lezake. Ahultasun horretarako CVE-2019-10931 identifikatzailea erabili da.
- SIMATIC WinCC DataMonitor web aplikazioak ahalbidetu lezake erasotzaile batek ASPX kode arbitrarioa kargatzea, eta horrela gailuaren konfidentzialtasun, integritate eta eskuragarritasunari eragitea. Ahultasun horretarako CVE-2019-10935 identifikatzailea erabili da.

Gainerako ahultasunetarako honako identifikatzaileak esleitu dira: CVE-2011-3389, CVE-2016-6329, CVE-2013-0169, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-10933.

Etiketak: Eguneraketa, Komunikazioak, Nabigatzailea, Pribatutasuna, Siemens, Ahultasuna

---

Sarbidearen kontrol desegokia Rockwell Automation-en PanelView 5510en

Argitalpen data: 2019/07/10

Garrantzia: Handia

Kaltetutako baliabideak:

2019ko martxoaren 13a baino lehen fabrikatutako PanelView 5510en bertsio guztiak, v4.003, v5.002 edo geroagoko bertsioetara eguneratuak izan ez badira.

Azalpena:

Rockwell Automation fabrikatzaileak berak eman du sarbidearen kontrol desegoki erako ahultasun baten berri. Kaltetutako gailura sarbidea lukeen urruneko erasotzaile batek ahultasun hau arrakastaz baliatuz gero, terminala abiaraz lezake eta fitxategien sistemara sarbidea lortu root pribilegioekin.

Konponbidea:

Ahultasun hau konpontzeko fabrikatzaileak gomendatzen du bere gailuak eguneratzea ondoko bertsioetara, erabilitako PanelView 5510 bertsioaren arabera:

- v4 erabiltzen duen PanelView 5510en kasuan, 4.003 edo geroagoko bertsioetara eguneratzea;
- v5 erabiltzen duen PanelView 5510en kasuan, 5.002 edo geroagoko bertsioetara eguneratzea.

Xehetasuna:

PanelView 5510 pantaila grafikora sarbidea lukeen urruneko eta autentifikatu gabeko erasotzaile batek, terminala abiaraz lezake eta gailuaren fitxategi sistemara sarbidea lortu root pribilegioekin. Ahultasun horretarako CVE-2019-10970 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Kredentzial barneratuak Emerson-en DeltaV Smart Switches-en

Argitalpen data: 2019/07/10

Garrantzia: Ertaina

Kaltetutako baliabideak:

- DeltaV Distributed Control System kudeaketa plataforma, honako bertsioak:
  - 11.3.x;
  - 12.3.x.

Azalpena:

Sanofiko Benjamin Crosasso ikertzaileak kritikotasun ertaineko ahultasun honen berri eman du. Erasotzaile batek administratzaile baimenekin sarbidea lor lezake DeltaV Smart Switches gailuetara.

Konponbidea:

Fabrikatzaileak eguneraketa partxeak aplikatzea gomendatzen du. Erabiltzaile erregistratuentzat daude eskuragarri DSN19003 (KBA# NK-1900-0808) artikuluan.

Xehetasuna:

Smart Switch Command Center-ek ez ditu aldatzen DeltaV Smart Switch-en administrazio kontuaren kredentzialak berau produkzioan jarri ondoren. Ondorioz, indarrean dagoen pasahitza modu lehenetsian betiko balio du. Ahultasun horretarako CVE-2018-11691 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Schneider Electric-en produktuetan

Argitalpen data: 2019/07/10

Garrantzia: Handia

Kaltetutako baliabideak:

- Zelio Soft, V5.2 bertsioa eta lehenagokoak;
- IGSS, 14. bertsioa eta lehenagokoak;
- Modicon M580 CPU - BMEP582040, V2.90 bertsioa baino lehenagoko guztiak;
- Modicon Ethernet Module BMENOC0301, V2.16 bertsioa baino lehenagoko guztiak.

Azalpena:

9SG Security Team-eko mdm eta rgod ikertzaileak, Zero Day Initiative-rekin (Trend Micro) lankidetzan, Schneider Electric-ek gailuek dituzten hainbat ahultasunen berri eman dute. Urruneko erasotzaile batek kodea exekuta lezake, ustekabeko itxiera eragin edo zerbitzuaren ukapen egoera sortu.

Konponbidea:

- Zelio Soft 5.3 bertsiora eguneratzea,
- IGSS ondoko bertsioetara eguneratzea:
  - 13.0.0.19140,
  - 14.0.0.19120.
- Modicon Ethernet Module BMENOC0301 2.16 bertsiora bertsiora eguneratzea,
- Modicon M580 - BMEP582040 2.90 bertsiora eguneratzea. Erreferentzien atala ikusi kaltetutako modeloarentzako egokia den eguneraketa deskargatzeko.

Xehetasuna:

- Ahultasunetako baten arrazoia da memoriaren bufferraren mugen barneko eragiketa desegokien murriztapenean dagoen akatsa. Akats horrek zerbitzuaren ukapen egoera eragin lezake Modicon Ethernet-en FTP zerbitzarian, 1020 byte baino gehiagoko datu luzerako FTP CWD komando bat jasotzean. CVE-2018-7838 identifikatzailea erreserbatu da.
- Mugez kanpoko idazketa erako ahultasun batek akatsa eragin lezake softwarean, mdb datu basean datuak manipulatzean. CVE-2019-6827 identifikatzailea erreserbatu da.
- Ahultasun baten arrazoia da baliabideen erabilpenean dagoen akatsa memoria askatu ondoren. Urruneko erasotzaile batek kodea exekuta lezake modu arbitrarioan. CVE-2018-6822 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Schneider Electric, Ahultasuna

Hainbat ahultasun Delta Electronics-en CNCSoft-en

Argitalpen data: 2019/07/12

Garrantzia: Handia

Kaltetutako baliabideak:

- CNCSoft ScreenEditor, 1.00.89 eta lehenagoko bertsioak.

Azalpena:

Natnael Samson ikertzaileak, Zero Day Initiative-rekin (Trend Micro) lankidetzan, bufferraren gainezkatze erako eta mugez kanpoko irakurketa erako ahultasun batzuen berri eman du. Urruneko erasotzaile batek ahultasun horiek arrakastaz baliatuz gero, kodea exekuta lezake, informazioa hedatu edo aplikazioa geldiarazi.

Konponbidea:

1.00.94 bertsiora eguneratzea.

Xehetasuna:

- Heap-en oinarritutako bufferraren gainezkatze erako hainbat ahultasun baliatuz, urruneko erasotzaile batek kode arbitrarioa exekuta lezake bereziki diseinatutako fitxategiak bidaliz, sarbidea egiaztatzen ez denez gero. Ahultasun horretarako CVE-2019-10982 identifikatzailea erreserbatu da.
- Mugez kanpoko irakurketa erako hainbat ahultasun baliatuz, informazioa zabal liteke proiektuko fitxategiak prozesatzerakoan erabiltzailearen sarbide datuak egiaztatzen ez direlako. Ahultasun horretarako CVE-2019-10992 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Ahultasuna Philips-en Holter 2010 Plus gailuetan

Argitalpen data: 2019/07/12

Garrantzia: Txikia

Kaltetutako baliabideak:

- Holter 2010 Plus, bertsio guztiak.

Azalpena:

Philipsek kritikotasun txikiko ahultasun bat aurkitu du bere produktu batean. Erasotzaile batek pribilegioen eskalatzea egin lezake kaltetutako ekipoan.

Konponbidea:

Philipsek ez du argitaratu ahultasuna konpontzen duen inolako eguneraketarik. Sistemarako sarbidea kontrolatzeko, bere bezeroei gomendatzen die roletan oinarritutako sarbide kontrolak ezartzea.

Xehetasuna:

Aldez aurretik eskuratu gabeko sistema aukerak gaitzea ahalbidetu dezakeen ahultasun bat aurkitu da. Erasotzaile batek, baldintza jakin batzuetan, sisteman pribilegioen eskalatzea egin lezake. Ahultasun horretarako CVE-2019-10968 identifikatzailea erreserbatu da.

Etiketak: Osasuna, Ahultasuna

Autentifikazio desegoki erako ahultasuna GEren Aestiva eta Aespire Anesthesia-n

Argitalpen data: 2019/07/15

Garrantzia: Ertaina

Kaltetutako baliabideak:

GE Aestiva eta GE Aespire, 7100 eta 7900 bertsioak.

Azalpena:

CyberMDXeko Elad Luz ikertzaileak autentifikazio desegoki erako ahultasun honen berri eman du. Ahultasun hori arrakastaz baliatuz gero urruneko erasotzaile batek kaltetutako gailuen parametroak alda litzake.

Konponbidea:

Ahultasuna duen gailu bat daukaten erakundeei GEk aholkatzen die terminal zerbitzari seguruak erabiltzea kaltetutako gailuen serie ataketara konektatzerakoan. GE Healthcare-ren asmoa da kaltetutako erabiltzaileei ahultasun honi buruzko eguneraketak eta segurtasun informazio osagarria eskaintzea bere webean.

Xehetasuna:

Autentifikazio desegoki erako ahultasun bat aurkitu da TCP/IP sare konfigurazio batera gehitutako terminal zerbitzari ez-seguru baten bidez konektatzen diren serieko gailuetan. Ahultasun hori baliatuz urruneko erasotzaile batek gailuaren konfigurazioa alda lezake eta alarmak isilarazi. Ahultasun horretarako CVE-2019-10966 identifikatzailea erabili da.

Etiketak: Osasuna, Ahultasuna

Autentifikazioari ihesa ABBren hainbat produktutan

Argitalpen data: 2019/07/16

Garrantzia: Handia

Kaltetutako baliabideak:

- CCLAS, 6.5 eta 6.6 bertsioak, mantenu bertsioak eta hotfix barne.
- Ellipse, 8.1etik 8.9ra bitarteko bertsioak, mantenu bertsioak barne.
- Ellipse, 9.0.0tik 9.0.6ra bitarteko bertsioak.

Azalpena:

ABBk larritasun altuko ahultasun bat aurkitu du. Sarbide baimenik gabeko erasotzaile batek aplikazioko datuak eskura litzake.

Konponbidea:

- CCLAS 6.6.0.4 eta 6.7 bertsioetara eguneratzea.
- Ellipse ondoko bertsioetara eguneratzea:
  - 8.5.25;
  - 8.6.25;
  - 8.7.23;
  - 8.8.19;
  - 8.9.19;
  - 9.0.7.

Xehetasuna:

Txostenak sortzeko mekanismoak dauka ahultasuna. Txosten bat sortzen denean diskoan gordetzen da, eta URL bat sortzen da txostena eskuratu ahal izateko erabiltzailearen interfazetik (UI). URL horrek ez ditu egiten beharrezkoak diren egiaztapenak eskaera egiten duen erabiltzailea autentifikatuta dagoela ziurtatzeko. Hori baliatuz URLra sarbidera lukeen erasotzaile batek txostena deskarga lezake.

Etiketak: Eguneraketa, Ahultasuna

Ahultasuna Johnson Controls erakundearen exacqVision zerbitzarian

Argitalpen data: 2019/07/19

Garrantzia: Ertaina

Kaltetutako baliabideak:

exacqVision zerbitzaria, 9.6 eta 9.8 bertsioak.

Deskribapena:

Applied Risk erakundeko Gjoko Kristic ikertzaileak tarteko kritikotasuna duen ahultasun honen berri eman du. Egiaztatu gabeko erasotzaile batek pribilegioetan gora egin lezake.

Konponbidea:

exacqVision zerbitzaria 19.03 bertsiora eguneratzea.

Xehetasuna:

Ahultasun horren arrazoia zera da: hainbat zerbitzuk dutela komatxo artean sartu gabeko zerbitzu-ibilbide bat. Erasotzaile batek kode arbitrarioa sar lezake sistemaren erroko ibilbidean, eta aplikazioa abiaraztean exekutatu. Ahultasun horretarako, CVE-2019-7590 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Mitsubishi Electric enpresaren FR Configurator2 sisteman

Argitalpen data: 2019/07/24

Garrantzia: Handia

Kaltetutako baliabideak:

FR Configurator2 1.16S bertsioan eta aurrekoetan.

Deskribapena:

Applied Risk enpresak XML External Entity (XXE) motako ahultasun baten berri eman du, batetik; eta, bestetik, baliabideen kontrolik gabeko kontsumoaren motako beste baten berri. Mitsubishi enpresaren FR Configurator2 sistemari eragiten diote.

Konponbidea:

Mitsubishi Electric erakundeak 1.17T bertsiora eguneratzea gomendatu du, hau da, azken bertsiora.

Xehetasuna:

- XML analizatzaileari emandako sarrera datuak ez dira aurretik sanitizatu. Horrek esan nahi du erasotzaile batek fitxategiak modu arbitrarioan irakur ditzakeela. Ahultasun horretarako, CVE-2019-10976 identifikatzailea erreserbatu da.
- Erasotzaile batek baimenik gabeko proiektu-fitxategi bat eman dezake (.frc2). Erabiltzaileak proiektu bat irekitzean, CPUaren nekea sortzen da, eta softwareak erantzuteari uzten dio, aplikazioa berrabiarazi arte. Horrek zerbitzu ukapena sortzen du. Ahultasun horretarako, CVE-2019-10972 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Bufferrak gainezka egin du National Renewable Energy Laboratory (NREL) erakundearen EnergyPlus sisteman

Argitalpen data: 2019/07/24

Garrantzia: Ertaina

Kaltetutako baliabideak:

- EnergyPlus, 8.6.0 bertsioa eta aurrekoak.

Deskribapena:

Karn Ganeshen ikertzaileak tarteko kritikotasuna duen ahultasun baten berri eman du. Ahultasun hori baliatuta, erasotzaile batek kode arbitrarioa exekutatu lezake, edota zerbitzu ukapena sortu.

Konponbidea:

Aplikazioaren bertsio honetara eguneratzea: (v9.0.1).

Xehetasuna:

Aplikazioak ez dauka mekanismo egokirik salbuespen kontrolagailu bat kode arbitrario bidez idaztea saihesteko. Aplikaziorako sarbidea daukan erasotzaile batek kode arbitrarioa exekutatu lezake, edota zerbitzu ukapen bat sortu. Ahultasun horretarako, CVE-2019-10974 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Wind River-en VxWorks sisteman

Argitalpen data: 2019/07/30

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- VxWorks:
  - 6.5 bertsioa eta 6.9.4 bertsioaren artekoak, biak barne;
  - 7 preSR620, SR540 eta SR610 bertsioak;
  - Interpeak-en sare independentearen sareko pila erabiltzen duten VxWorks bertsioak;
  - Seguru aski, jarraituak ez diren bertsio guztiak.

Deskribapena:

RTOS VxWorks sistemari eragiten dioten 11 ahultasun identifikatu dira, bufferraren gainezkatze eta memoriaren usteltze motakoak. Erasotzaile batek modu arbitrarioan exekutatu lezake kodea, zerbitzu ukapena sortu edota informazio ihesa eragin. VxWorks erabiltzen duten gailuetako batzuk honakoak dira: SCADA gailuak, industria kontrolagailuak, monitorizaziorako gailu medikoak, erresonantzia magnetikoko makinak, firewall, VoIP telefonoak eta inprimagailuak.

Konponbidea:

Wind River etxeak VxWorks erakundearen 7 SR620 bertsioa argitaratu du, ahultasun horiek konpontzeko. Informazio gehiago lortzeko, jo laguntza emateko orrialde nagusira.

Xehetasuna:

Larritasun kritikoa duten ahultasunek honakoak eragin ditzakete:

- Bufferraren gainezkatzea, gailu horretara bereziki diseinatutako IP/DHCP paketeak bidaliz. Gailuak ez du horretarako aplikazio edo konfigurazio espezifikorik eskatzen. Hori baliatuta, kode arbitrarioaren exekuzioa eman daiteke. Ahultasun horretarako, CVE-2019-12256 identifikatzailea erreserbatu da.
- Memoria usteltzea, TCP punteroaren eremua modu desegokian erabilita. Erasotzaile batek eremu hori erabil dezake TCP portuaren bidez konektatu eta kodea modu arbitrarioan exekutatzeko. Ahultasun horietarako CVE-2019-12255 eta CVE-2019-12260 identifikatzaileak erreserbatu dira.

Gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2019-12257, CVE-2019-12258, CVE-2019-12261, CVE-2019-12262, CVE-2019-12263, CVE-2019-12264, CVE-2019-12259 eta CVE-2019-12265.

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

Hainbat ahultasun 3S-Smart Software Solutions GmbH erakundearen CODESYS produktuetan

Argitalpen data: 2019/07/30

Garrantzia: Handia

Kaltetutako baliabideak:

- CODESYS Control,honako sistemetarako:
  - para BeagleBone;
  - para emPC-A/iMX6;
  - para IOT2000;
  - para PFC100;
  - para PFC200;
  - para Raspberry Pi;
  - para Linux;
  - RTE V3;
  - RTE V3 (para Beckhoff CX);
  - V3 Runtime System Toolkit;
  - Win V3 (CODESYS Development System setup sistemaren parte ere);
- CODESYS V3 Simulation Runtime (CODESYS Development System sistemaren parte);
- CODESYS HMI V3;
- CODESYS V3 Safety SIL2;
- CODESYS Gateway V3;
- CODESYS Development System V3 sistemaren aldaera guztiak, V3.5.15.0 bertsioaren aurrekoetan.

Deskribapena:

Kritikotasun handiko hainbat ahultasun identifikatu dira, CODESYS produktuei eragiten dietenak. Ahultasun horiek baliatuta, urrutiko erasotzaile batek zerbitzu ukapena eragin dezake, baita kode arbitrarioaren exekuzioa, informazioa erakustea edota kredentzialen bahiketa ere.

Konponbidea:

3S-Smart Software Solutions GmbH erakundeak hainbat eguneratze garatu ditu kaltetutako gailuentzat, software deskargarako zentroan.

Xehetasuna:

- CODESYS Runtime sistemaren lineako erabiltzaileen kudeaketak azpi-objektuetarako sarbide desegokia eman dezake, baita konektatutako erabiltzaileak horietara sartzeko baimenik jasotzen ez badu ere. Ahultasun horretarako, CVE-2019-9008 identifikatzailea erreserbatu da.
- CODESYS garapen sistemak eduki maltzurrak erakutsi edota exekutatu litzake dokumentazio liburutegian, aurretik baliagarritasuna egiaztatu aurretik.
- Bereziki diseinatutako eskaera batek errore ez kontrolatua eragin dezake kaltetutako CODESYS produktuetan. Urrutiko erasotzaile batek edota zerbitzuaren ukapen baldintza bat sortu dezake.
- Ahultasun horretarako, CVE-2019-9009 identifikatzailea erreserbatu da.Konfiantzazko OPC UA bezero batek bidalitako eskaera batek puntero baliogabe baten erreferentzia sor lezake. Horrek zerbitzu ukapenaren egoera ekar lezake.
- TLS zifratuan oinarritutako CODESYS komunikaziorik erabiltzen ez bada, kredentzialak ez dira behar bezain babestuta egongo garraio-prozesuan zehar. PCL komunikazioetarako sarbidea daukan erasotzaile batek erabiltzailearen kredentzialak lortu litzake. Ahultasun horretarako, CVE-2019-9013 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna

Ahultasuna Bus CAN sarearen inplementazioan

Argitalpen data: 2019/07/31

Garrantzia: Handia

Kaltetutako baliabideak:

Bus CAN sareak erabiltzen dituen aireontziak.

Deskribapena:

Rapid7 erakundeak ahultasun bat atzeman du aireontzietako Bus CAN sarearen inplementazioan. Ahultasun horri esker, aireontzirako sarbide fisikoa daukan erasotzaile batek datu faltsuak injektatu litzake, hegazkin sistemetan irakurketa okerrak egiteko aukerarekin.

Konponbidea:

Honako neurriak hartzea gomendatu da:

- Aireontzien jabeei: Hegazkinetarako sarbidea mugatu, ahal den neurrian:
- Aireontzien fabrikatzaileei: Bus CAN sareen inplementazioa errebisatzea, eraso fisikoaren bektorea konpentsatzeko. Automobilgintzaren industrian aurrerapenak eman dira, eta Bus CAN sistemen antzeko eraso fisikoak saihesteko babesak hobetu dira. Segurtasun neurriak baloratu beharko lirateke, hala nola filtratzea, zerrenda zurien erabilera edota Bus CAN sarearen segregazio espezifikoa.

Xehetasuna:

Aireontzirako sarbide fisikoa daukan erasotzaile batek gailu bat konektatu lezake Bus CAN sarean eta gero datu faltsuak injektatu. Horren ondorioz, irakurketa okerrak emango lirateke aireontziaren hegazkin sistemetan. Ikertzaileek adierazi dute motorraren telemetria irakurketak, brujula, altitudea, airearen abiadura eta eraso angelua manipulatu egin daitezkeela pilotuari neurketa faltsuak bidaltzeko. Horren ondorioz, aireontziaren kontrola gal daiteke.

Etiketak: Komunikazioak, Ahultasuna

Prima Systems erakundearen FlexAir sistemaren

ahultasunak

Argitalpen data: 2019/07/31

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Prima FlexAir, 2.3.38 bertsioa eta aurrekoak.

Deskribapena:

Applied Risk enpresako Gjoko Krstic ikertzaileak hainbat ahultasunen berri eman du: sistema eragilearen komando injekzio motakoak, fitxategi maltzurren mugarik gabeko karga, CSRF, balio aleatorioen espazio txikia, XSS, baimenik gabeko erabiltzaileei babes fitxategiak erakustea, egiaztapen desegokia eta kredentzial barneratuen erabilera. Ahultasun horiek baliatuta, urrutiko erasotzaile batek sistema eragilearen komandoak exekutatu litzake, fitxategi maltzurrak kargatu, ekintzak administrari baimenekin burutu, erabiltzailearen nabigatzailean kode arbitrarioa exekutatu, sarbide kredentzialak lortu, egiaztatzeari ihes egin eta sistemarako sarbide osoa izan.

Konponbidea:

Prima Systems erakundeak FlexAir sistemaren 2.5.12 bertsioa argitaratu du, ahultasun horiek konpontzeko.

Xehetasuna:

Ondoren, kritikotasun handieneko ahultasunak zehaztu dira:

- Sistema eragilearen komando injekzioa: Aplikazioak modu desegokian neutralizatzen ditu espazio elementuak. Elementu horiek sistema eragilearen komandoa aldatzeko aukera emango lukete, osteko osagai bati bidaltzen zaionean; hori baliatuz, erasotzaile batek komandoak exekutatu litzake zuzenean, sistema eragilean. CVE-2019-7670 kodea esleitu zaio ahultasun horri.
- Fitxategi maltzurrak mugarik gabe kargatzea:
  - Fitxategiak kargatzean luzera modu desegokian balioztatzen bada, urrutiko erasotzaile batek aplikazio maltzurrak kargatu eta exekutatu litzake web aplikazioaren erroan, administrari baimenekin. Ahultasun horretarako, CVE-2019-7669 identifikatzailea esleitu da.
  - Aplikazioaren bidez, Python sistemako script arbitrarioak karga daitezke, kontrolagailu zentral nagusiaren konfigurazioa egin bitartean. Script horiek administrari moduan exekutatu daitezke zuzenean, eta ez web zerbitzariaren erabiltzaile moduan. Horrela izanik, egiaztatutako erasotzaile batek sistemarako sarbide erabatekoa izan dezake. Ahultasun horretarako, CVE-2019-9189 identifikatzailea esleitu da.
- Babes fitxategiak erakustea baimenik gabeko erabiltzaileei: Aplikazioak datu-baseko fitxategiak sortzen ditu, erraz asmatzeko moduko izenekin. Horrela, erasotzaile batek fitxategiaren izena aurreikus dezake indarrezko eraso baten bidez. Erasotzaile batek ahultasun hori baliatu dezake eta datu-basearen fitxategia lortu saio hasierako informazioarekin. Horrela, egiaztatzea saihestu eta sistemarako sarbide erabatekoa lortu dezake. Ahultasun horretarako, CVE-2019-7667 identifikatzailea esleitu da.
- Egiaztatze okerra: Aplikazioaren bidez, egiaztatze egoki bat egin daiteke, pasahitzaren hash MD5 balioa erabiliz. Horrela, erasotzaile batek saioa hasteko datu-baserako sarbidea izan dezake, pasahitzik deszifratu beharrik gabe. Ahultasun horretarako, CVE-2019-7666 identifikatzailea esleitu da.
- Kredentzial barneratuen erabilera: Web interfazearen flash bertsioak erabiltzaile eta pasahitz barneratuak ditu; horrela izanik, egiaztatutako erasotzaile batek pribilegioetan gora egin lezake. Ahultasun horretarako, CVE-2019-7672 identifikatzailea esleitu da.

Gainerako ahultasunetarako, identifikatzaile batzuk esleitu dira: CVE-2019-7280, CVE-2019-7281 eta CVE-2019-7671.

Etiketak: Eguneraketa, Ahultasuna