2019ko Apirilaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Hainbat ahultasun Advantech-en WebAccess-en

Argitalpen data: 2019/04/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- WebAccess/SCADA, 8.3.5 eta lehenagoko bertsioak.

Azalpena:

Mat Powell eta Natnael Samson ikertzaileek, Trend Micro Zero Day Initiative-rekin elkarlanean, Advantech-en WebAccess softwareari eragiten dioten era ezberdinetako hainbat ahultasun aurkitu dituzte: komandoen injekzioa, bufferraren gainezkatzea eta sarbidearen kontrol okerra.

Konponbidea:

- WebAccess 8.4.0 bertsiora eguneratzea.

Xehetasuna:

Erasotzaile batek ondokoa egin lezake:

- Komandoak injektatzea, erabiltzaileak emandako datuen baliozkotzean dagoen akats baten eraginez. Ahultasun horretarako CVE-2019-6552 identifikatzailea erreserbatu da.
- Kode arbitrarioa exekutatzea, pilan oinarritutako bufferraren gainezkatzearen eraginez, erabiltzaileak emandako datuen luzeraren baliozkotzearen akats bat dela eta. Ahultasun horretarako CVE-2019-6550 identifikatzailea erreserbatu da.
- Zerbitzuaren ukapen egoera eragitea, sarbidearen kontrol okerraren ahultasun bat dela eta. Ahultasun horretarako CVE-2019-6554 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, SCADA, Ahultasuna

Hainbat ahultasun Bosch-en produktuetan

Argitalpen data: 2019/04/04

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Access Easy Controller (AEC), bertsio hauek baino lehenagokoak: 2.1.8.5 (hau barne), 2.1.9.0, 2.1.9.1 eta 2.1.9.3
- Access Professional Edition (APE), 3.0 baino lehenagoko bertsioak eta 3.0tik 3.7ra bitartekoak (soilik VSDK osagaia instalatuta baldin badago)
- Bosch DIVAR IP 2000 eta 5000
- Bosch DIVAR IP 3000
- Bosch DIVAR IP 7000, Gen1 eta Gen2
- Bosch Video Client (BVC)
- Bosch Video Management Systems (BVMS), 6.0, 6.5, 7.0, 7.5, 8.0 eta 9.0 bertsioak
- Bosch Video Streaming Gateway (VSG)
- Building Integration System (BIS), 2.2tik 4.4ra bitarteko bertsioak, 4.5, 4.6 eta 4.6.1 barne
- Configuration Manager
- Video Recording Manager (VRM)
- Video SDK (VSDK)

Azalpena:

Bosch produktuei eragiten dieten lau ahultasun aurkitu dira, horietako batzuk Adrián Quirós Godoy ikertzaile independenteak

aurkitutakoak. Horietatik bi kritikoak izanik, ahultasunak era hauetakoak dira: bufferraren gainezkatzea, sarbidearen kontrol desegokia, birbideratze irekia eta direktorio jauzia. Ahultasun horiek arrakastaz baliatuz gero, baimenik gabeko urruneko erasotzaile batek RCP komandoen injekzioaren bidez sisteman irakurri eta idatz lezake, direktorio eta fitxategietara sarbidea lortu eta sisteman kode arbitrarioa exekutatu.

Konponbidea:

- Ohartarazpen kritikoen kasuan fabrikatzaileak gomendatzen du kaltetutako produktuen softwarea partxeatutako bertsio batera eguneratzea, ondoko ohartarazpenen arabera: BTren sarbide desegokiaren kontrolari buruzko ohartarazpenaren eranskina eta BTren bufferraren gainezkatzeari buruzko ohartarazpenaren eranskina. Partxeak eta horiek instalatzeko prozedurak Bosch-en deskargen gunean aurki daitezke.
- Arazoa konpontzen duen eguneraketarik argitaratu ez bada edo ezin bada eguneratu, arazoa arintzeko *firewall*-ari arauak gehitzea aholkatzen da.

Xehetasuna:

- RCPren aztertzailean (parser) bufferraren gainezkatzea: erasotzaile batek urrunetik kodea exekuta lezake sarreraren tamaina ez delako egiaztatzen. Ahultasun horretarako CVE-2019-6957 kodea erreserbatu da.
- Sarbidearen kontrol desegokia: RCP atakak autentifikaziorik gabeko sarbideak ahalbidetzen ditu. Urruneko erasotzaile batek bideo baten datuak ezabatu edo irakur litzake. Ahultasun horretarako CVE-2019-6958 kodea erreserbatu da.
- Birbideratze irekia: urruneko erasotzaile batek erabiltzaileak birbidera litzake asmo gaiztoko edukia duen URL batera. Ahultasun horretarako CVE-2019-8951 kodea erreserbatu da.
- Direktorio jauzia: erasotzaile batek fitxategien sistemetara eta murriztutako fitxategi edo direktorioetara sarbidea lor lezake. Ahultasun horretarako CVE-2019-8952 kodea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Memoriaren hondatze erako ahultasuna Omron-en CX-Programmer-en

Argitalpen data: 2019/04/05

Garrantzia: Ertaina

Kaltetutako baliabideak:

- CX-Programmer, 9.70 bertsioa eta lehenagokoak.
- Common Components, 2019ko urtarrileko bertsioa eta lehenagokoak.

Azalpena:

Source Incite-ko Esteban Ruiz ikertzaileak, Trend Micro-ko Zero Day Initiative-rekin lankidetzan, memoria askatu ondoreneko baliabideen erabilpen erako ahultasun bat aurkitu du Omron-en CX-Programmer-en.

Konponbidea:

- CX-Programmer, 9.71 bertsioa
- Common Components, 2019ko apirileko bertsioa

Xehetasuna:

- Erasotzaile batek bereziki manipulatutako proiektu fitxategi bat erabil lezake aplikazioaren pribilegioekin kodea ustiatu eta exekutatzeko, askatutako memoriarako erreferentziak baliatuz. Ahultasun horretarako CVE-2019-6556 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Rockwell Automation-en produktuetan

Argitalpen data: 2019/04/05

Garrantzia: Handia

Kaltetutako baliabideak:

- Allen-Bradley Stratix 5400, 5100 eta 5700, 15.2(6)E2a baino lehenagoko bertsioak
- Allen-Bradley ArmorStratix 5700, 15.2(6)E2a baino lehenagoko bertsioak
- Allen-Bradley Stratix 8000, 15.2(6)E0a baino lehenagoko bertsioak
- Allen-Bradley Stratix 8300, 15.2(4)EA7 baino lehenagoko bertsioak
- Modelos Allen-Bradley Stratix 5950:
  - 1783-SAD4T0SBK9
  - 1783-SAD4T0SPK9
  - 1783-SAD2T2SBK9
  - 1783-SAD2T2SPK9

Azalpena:

Rockwell Automation-ek era ezberdinetako hainbat ahultasunen berri eman du: baliabideen kontrolik gabeko kontsumoa, baliabideen kudeaketan akatsak eta sarrera datuen baliozkotze desegokia. Ahultasun horiek arrakastaz baliatuz gero, baimenik gabeko urruneko erasotzaile batek zerbitzuaren ukapen egoera eragin lezake gailuan edo PTP (*Precision Time Protocol*) zerbitzuan.

Konponbidea:

Fabrikatzaileak gomendatzen du kaltetutako produktuen softwarea ondoko bertsioetara (edo berriagoetara) eguneratzea:

- FRN 15.2(6)E2a:
  - Allen-Bradley Stratix 5400
  - Allen-Bradley Stratix 5410
  - Allen-Bradley Stratix 5700
  - Allen-Bradley ArmorStratix 5700
  - Allen-Bradley Stratix 8000
- FRN 15.2(4)EA7:
  - Allen-Bradley Stratix 8300
- Kaltetutako Allen-Bradley Stratix 5950 produktuen kasuan, modu lehenetsian IPsec zerbitzua desgaiturik dutenez, fabrikatzaileak gomendatzen du VPN IPsec konexiorik ez erabiltzea. Era berean firewall arauak, ACLak eta kaltetutako gailuak agerian jartzearekin zerikusia duten neurriak erabiltzea gomendatzen du.

Xehetasuna:

- Autentifikaziorik gabeko urruneko erasotzaile batek datu baliogabeak bidal liezazkioke Cisco Network Plug and Play-ren agenteari. Horrela memoria galtzea eragingo litzateke eta, ondorioz, kaltetutako gailua berrabiaraztea, zerbitzuaren ukapen egoera (DoS) sortuz. Ahultasun horretarako CVE-2018-15377 kodea erabili da.
- Autentifikaziorik gabeko erasotzaile batek bereziki diseinatutako OSPFv3 pakete bat bidal lezake kaltetutako gailu batean berrabiatzea eragiteko, eta ondorioz gailu berean zerbitzuaren ukapen egoera sortzeko. Ahultasun horretarako CVE-2018-0466 kodea erabili da.
- Autentifikaziorik gabeko urruneko erasotzaile batek Cisco XEren web framework-ean gaizki sortutako HTTP pakete bat bidal lezake, modu horretan bufferraren gainezkatzea eraginez eta, ondorioz, gailuan zerbitzuaren ukapen egoera sortuz. Ahultasun horretarako CVE-2018-0470 kodea erabili da.
- Autentifikaziorik gabeko urruneko erasotzaile batek gaizki sortutako IPsec paketeak bidal liezazkioke kaltetutako gailu bati. Horrela bere berrabiatzea eragingo luke eta, ondorioz, zerbitzuaren ukapen egoera. Ahultasun horretarako CVE-2018-0472 kodea erabili da.
- Autentifikaziorik gabeko urruneko erasotzaile batek pertsonalizatutako PTP pakete bat bidal liezaioke kaltetutako gailu bati. Horrela PTPn zerbitzuaren ukapen egoera eragingo luke eta, ondorioz, sarean denboraren desinkronizazioa. Ahultasun horretarako CVE-2018-0473 kodea erabili da.
- Autentifikaziorik gabeko erasotzaile batek Cisco Recovery Protocol paketeen tasa altu bat bidal liezaioke kaltetutako gailu bati, horrela bere memoria betez eta ondorioz zerbitzuaren ukapen egoera sortuz. Ahultasun horretarako CVE-2018-15373 kodea erabili da.
- Autentifikaziorik gabeko urruneko erasotzaile batek asmo gaiztoko IPsec paketeak bidal liezazkioke kaltetutako gailu bati. Horrela bere berrabiatzea eragingo luke eta, ondorioz, zerbitzuaren ukapen egoera. Ahultasun horretarako CVE-2018-0467 kodea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Ahultasuna SmartLinx Neuron 2 osasun gailuetan

Argitalpen data: 2019/04/09

Garrantzia: Handia

Kaltetutako baliabideak:

- SmartLinx Neuron 2, 6.9.1 bertsioa

Azalpena:

Talos Intelligence-ko Patrick DeSantis ikertzaileak ingurune murriztuaren ihes erako ahultasuna aurkitu du Capsule Technologies-en SmartLinx Neuron 2 produktuan, bizi zeinuen datuak automatikoki biltzea ahalbidetzen duen ordenagailu kliniko mugikor bat. Hori baliatuz erasotzaile batek ospitale baten barne sareko konfiantzazko gailu baten kontrol osoa eskura lezake.

Konponbidea:

- 10.1 bertsiora eguneratzea.

Xehetasuna:

- Gailu honek kiosk mode izeneko ingurune murriztu bat du. Horrek ekiditen du erabiltzaileak exekutatzen ari diren aplikazioetatik atera ahal izatea eta azpiko sistema eragilera sartu ahal izatea. Posible da USB teklatu bat edo HID motako beste gailu batzuk konektatzea eta teklatuaren pultsazio segida baten bidez ingurune murriztu horretatik ateratzea, eta horrela Microsoft Windows-en sistema eragilera sarbidea lortzea administratzaile baimenekin. Sarbide hori baliatuz erasotzaile batek ospitale baten barne sareko konfiantzazko gailu baten kontrol osoa eskura lezake. Ahultasun horretarako CVE-2019-5024 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna

Hainbat ahultasun Siemens produktuetan

Argitalpen data: 2019/04/09

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- RUGGEDCOM ROX II, V2.13.0 baino lehenagoko bertsio guztiak
- SINEMA Remote Connect Client, V2.0 HF1 baino lehenagoko bertsio guztiak
- SINEMA Remote Connect Server, V2.0 baino lehenagoko bertsio guztiak
- Spectrum PowerTM 4: Web Office Portal-dun bertsioa
- SIMATIC CP443-1 OPC UA, bertsio guztiak
- SIMATIC ET 200 Open Controller CPU 1515SPPC2, bertsio guztiak
- SIMATIC IPC DiagMonitor, bertsio guztiak
- SIMATIC NET PC Software, bertsio guztiak
- SIMATIC RF188C, bertsio guztiak

- SIMATIC RF600R, bertsio guztiak
- SIMATIC S7-1500 CPU family, V2.5 bertsioa baino lehenagoko guztiak
- SIMATIC S7-1500 Software Controller, V2.5 bertsioa baino lehenagoko guztiak
- SIMATIC WinCC OA, V3.15-P018 bertsioa baino lehenagoko guztiak
- SIMATIC WinCC Runtime Advanced, Comfort, HSP Comfort eta Mobile, bertsio guztiak
- SINEC-NMS, bertsio guztiak
- SINEMA Server, bertsio guztiak
- SINUMERIK OPC UA Server, V2.1 bertsioa baino lehenagoko guztiak
- TeleControl Server Basic, bertsio guztiak
- CP1604, bertsio guztiak
- CP1616, bertsio guztiak
- SIMATIC RF185C, bertsio guztiak
- SIMATIC CP443-1 eta CP343-1 Advanced, bertsio guztiak
- SIMATIC CP443-1 OPC UA eta CP443-1 Advanced, bertsio guztiak
- SIMATIC ET 200 SP Open Controller CPU1515SP PC, V2.1.6 bertsioa baino lehenagoko guztiak
- SIMATIC ET 200 SP Open Controller CPU1515SP PC2, bertsio guztiak
- SIMATIC HMI Comfort Outdoor Panels 7" & 15", bertsio guztiak
- SIMATIC HMI Comfort Panels 4" - 22", bertsio guztiak
- SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 eta KTP900F, bertsio guztiak
- SIMATIC IPC DiagMonitor, bertsio guztiak
- SIMATIC RF181-EIP, RF182C, RF186C, RF188C eta RF600R, bertsio guztiak
- SIMATIC S7-1500 CPU family, bertsio guztiak
- SIMATIC S7-1500 Software Controller, bertsio guztiak
- SIMATIC S7-300 CPU family, V3.X.16 bertsioa baino lehenagoko guztiak
- SIMATIC S7-400 PN (F barne), V6 eta ondorengoak, bertsio guztiak
- SIMATIC S7-400 PN/DP V7 (F barne), bertsio guztiak
- SIMATIC S7-PLCSIM Advanced, bertsio guztiak
- SIMATIC Teleservice Adapter IE Advanced, Basic eta Standard, bertsio guztiak
- SIMATIC WinAC RTX 2010, bertsio guztiak
- SIMATIC WinCC Runtime Advanced, bertsio guztiak
- SIMOCODE pro V EIP, bertsio guztiak
- SIMOCODE pro V PN, bertsio guztiak
- SINAMICS G130 V4.6, bertsio guztiak
- SINAMICS G130 V4.7 eta SP1, bertsio guztiak
- SINAMICS G130 V4.8, 4.8 HF6 baino lehenagoko bertsio guztiak
- SINAMICS G130 V5.1, bertsio guztiak
- SINAMICS G130 V5.1 SP1, V5.1 SP1 HF4 baino lehenagoko bertsio guztiak
- SINAMICS G150 V4.6, V4.7 eta V4.7 SP1, bertsio guztiak
- SINAMICS G150 V4.8, V4.8 HF6 baino lehenagoko bertsio guztiak
- SINAMICS G150 V5.1, bertsio guztiak
- SINAMICS G150 V5.1 SP1, V5.1 SP1 HF4 baino lehenagoko bertsio guztiak
- SINAMICS S120 V4.6, V4.7 eta V4.7 SP1, bertsio guztiak
- SINAMICS S120 V4.8, V4.8 HF6 baino lehenagoko bertsio guztiak
- SINAMICS S120 V5.1, bertsio guztiak
- SINAMICS S120 V5.1 SP1, V5.1 SP1 HF4 baino lehenagoko bertsio guztiak
- SINAMICS S150 V4.6, V4.7 eta V4.7 SP1, bertsio guztiak
- SINAMICS S150 V4.8, V4.8 HF6 baino lehenagoko bertsio guztiak
- SINAMICS S150 V5.1, bertsio guztiak
- SINAMICS S150 V5.1 SP1, V5.1 SP1 HF4 baino lehenagoko bertsio guztiak
- SINAMICS S210 V5.1 eta V5.1 SP1, bertsio guztiak
- SITOP Manager, PSU8600, UPS1600, bertsio guztiak
- TIM 1531 IRC, bertsio guztiak

Azalpena:

Applied Risk enpresak kudeatu du CVE-2019-6579 identifikatzailea duen ahultasuna, Siemens ProductCERTeko ekipoarekin lankidetzan. Gainerako ahultasunak fabrikatzaileak berak kudeatu ditu. Aurkitutako ahultasunak era hauetakoak dira: Quagga BGP deabruaren manipulazioa, bufferraren gainezkatzea, baimenik gabeko sarbidea eta bereziki diseinatutako paketeen bidalketa. Horiek baliatuz erasotzaile batek kodea exekuta lezake urrunetik, zerbitzuaren ukapen egoerak eragin eta kaltetutako gailuetan konfigurazio aldaketak egin.

Konponbidea:

- RUGGEDCOM ROX II gailuen kasuan, V2.13.0 bertsiora eguneratzea gomendatzen da. Arintze neurri modura, Siemensek bere bezeroei aholkatzen die ondoko ekintzak aplikatzea:
-
    - BGP bideen zerbitzua desgaitzea, erabiltzen ari ez bada.
    - BGP pasahitzak konfiguratzea, elkarren gertukoak diren BGPak autentifikatzeko.
- SINEMA Remote Connect Client gailuen kasuan, V2.0 HF1 bertsiora eguneratzea gomendatzen da.
- SINEMA Remote Connect Server gailuen kasuan, V2.0 bertsiora eguneratzea gomendatzen da. Arintze neurri modura, Siemensek bere bezeroei aholkatzen die ondoko ekintzak aplikatzea:
-
    - NTLM autentifikazioa desgaitzea, CVE-2018-16890 eta CVE-2019-3822 ahultasunen eragina arintzeko.
    - SMTP zerbitzua desgaitzea, CVE-2019-3823 ahultasunaren eragina arintzeko.
    - Egokiak diren arintze estrategiak aplikatzea.
- Spectrum PowerTM 4 sistemen kasuan, bf-47456_PE_WOP_fix bugfix-a ezabatzea gomendatzen da. Aurrekoez gain, Siemensek gomendatzen du web zerbitzaria desgaitzea edo bertarako sarbidea mugatzea kanpoko suebaki baten bidez.
- CVE-2019-6575 eta CVE-2019-6568 identifikatzaileak dituzten ahultasunek kaltetutako gainerako gailuen kasuan, Erreferentziak atalean eskainitako loturei dagozkien Siemensen abisuen WORKAROUNDS AND MITIGATIONS sailak bisitatzea.

Xehetasuna:

- Autentifikaziorik gabeko erasotzaile lokal batek, 80/TCP eta 443/TCP ataken bidez zerbitzarirako sarbidea badu, komandoak injekta litzake eta horrela administratzaile pribilegioekin exekuta litzake. Ahultasun horretarako CVE-2019-6579 identifikatzailea erreserbatu da.
- Erasotzaile batek BGP UPDATE mezuak ordezka litzake eta memoriaren askapen bikoitza balia lezake zerbitzuaren ukapen egoera eragiteko edo kode arbitrarioa exekutatzeko. Ahultasun horretarako CVE-2018-5379 identifikatzailea erabili da.
- Gainerako ahultasunetarako honako identifikatzaileak esleitu dira: CVE-2018-5380, CVE-2018-5381, CVE-2019-6568, CVE-2018-14618, CVE-2018-16890 eta CVE-2019-3822.Erreserbatutako identifikatzaileak, aldiz, honakoak dira: CVE-2019-6575 eta CVE-2019-6570.

Etiketak: Siemens, Ahultasuna

Ahultasuna Schneider-en Modbus Serial Driver-en

Argitalpen data: 2019/04/10

Garrantzia: Handia

Kaltetutako baliabideak:

Modbus Serial Driver, ondoko bertsioetan:

- 64 bit-eko Windows Sistema Eragilerako, V3.17 IE 37 eta lehenagokoak.
- 32 bit-eko Windows Sistema Eragilerako, V2.17 IE 27 eta lehenagokoak.
- Driver Suite, V14.12 eta lehenagoko bertsioak.

Azalpena:

Dragos-eko Reid Wightman ikertzaileak kanpotik kontrolatutako baliabiderako erreferentzien erako ahultasun bat aurkitu du Modbus Serial Driver produktuetan. Hori baliatuz erasotzaile batek sarbidea lor lezake sistemaren barnean.

Konponbidea:

- Ondoko partxea aplikatzea.

Xehetasuna:

- Kanpotik kontrolatutako baliabide baterako erreferentziak baliatuz, erasotzaile batek sarbidea lor lezake soilik pribilegiodun erabiltzaileentzat eskuragarri dauden sistemako fitxategietara idazketa baimenekin. Ahultasun horretarako CVE-2018-7824 kodea erreserbatu da.

Etiketak: Schneider Electric, Ahultasuna

Kontrolatu gabeko sarbidea bideetara Sprecher Automation-en SPRECON osagaietan

Argitalpen data: 2019/04/10

Garrantzia: Txikia

Kaltetutako baliabideak:

- SPRECON-E-C/P *firmwarea*, 8.52tik 8.62ra bitarteko bertsioak, PU244x hardwarearen aldaeretan.

Azalpena:

Sprecher Automation-ek path traversal erako ahultasun baten berri eman du. Kaltetutako gailuak dauden sarera sarbidea lukeen erasotzaile batek, era berean web aplikazioan autentifikatuta baldin badago, informazio sentikorra duten fitxategiak deskarga eta kontsulta litzake.

Konponbidea:

- Eskuragarri dagoen *firmware*aren azken bertsioetara eguneratzea gomendatzen da (8.52g eta 8.56f), ahultasun horiek konpontzen baitituzte.
- Rolek kontrolatutako sarbidea (*RBAC*) aktibatuta badago, ezin da ahultasun hau baliatu erabiltzaile kredentzial baliagarriak izan gabe. Fabrikatzaileak aholkatzen du erabiltzaileen autentifikazioa beti izatea aktibatuta interfaze guztietan. Edozein kasutan, sarea segmentatzea gomendatzen da, interfaze bakoitzaren interfazeak babesteko.

Xehetasuna:

- Ahultasun hau *Path Traversal* erakoa da. Ahultasunak kaltetutako gailura web sarbidea lukeen erasotzaile batek fitxategietarako sarbidea lor lezake web zerbitzariaren baimenekin (www-data).

Etiketak: Eguneraketa, Ahultasuna

Dokumentatu gabeko zerbitzurako sarbidea WAGOren gailuetan

Argitalpen data: 2019/04/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- 14. bertsioa baino lehenagoko firmwarea duten 750-88x serieak:
-
  - 750-330
  - 750-352/
  - 750-829
  - 750-831
  - 750-852
  - 750-880/
  - 750-881
  - 750-882
  - 750-884/

    - 750-885
    - 750-889
- 750-87x serieak
    - FW06 bertsioa baino lehenagoko firmwaredun 750-830.
    - FW08 bertsioa baino lehenagoko firmwaredun 750-849.
    - FW11 bertsioa baino lehenagoko firmwaredun 750-871.
    - FW07 bertsioa baino lehenagoko firmwaredun 750-872.
    - FW07 bertsioa baino lehenagoko firmwaredun 750-873.

Azalpena:

CERT-Bund-eko Jörn Schneeweisz segurtasun ikertzaileak koordinatu du ahultasun hau CERT-Bund-ekin berarekin batera. Barneratutako pasahitzen erabilpen erako ahultasun hau baliatuz, urruneko erasotzaile batek gailuaren edo bere aplikazioaren konfigurazioak alda litzake.

Konponbidea:

- Gailua eskuragarri dagoen firmwarearen azken bertsiora eguneratzea gomendatzen da, kaltetutako gailuaren eta firmware ahularen bertsioaren arabera.
- Firmwarearen bertsioa eguneratzerik ez badago ondokoa egitea gomendatzen da:
-
    - Web zerbitzari aktiboarekin kaltetutako gailua dagoen sarerako sarbidea murriztea.
    - Gailurako sarbidea murriztea.
    - Internetetik gailurako sarbide zuzenik ez eskaintzea.

Xehetasuna:

- Barneratutako pasahitzen erabilpena baliatuz, erasotzaile batek gailuaren konfigurazioa alda lezake eta webaren administraziora pribilegiodun sarbidea lortu. Horrela gailuko beste erabiltzaile batzuk blokea litzake, aldez aurretik itxitako sare atakak ireki, FTP zerbitzua erabili, aplikazioa trukatu edo ezabatu. Ahultasun horretarako CVE-2019-10712 identifikatzailea erreserbatu da.

Etiketak: Nabigatzailea, Ahultasuna

Buffer gainezkatzeak Delta Industrial Automation-en CNCSoft-en

Argitalpen data: 2019/04/17

Garrantzia: Handia

Kaltetutako baliabideak:

- CNCSoft ScreenEditor, 1.00.88 eta lehenagoko bertsioak.

Azalpena:

Natnael Samson segurtasun ikertzaileak eta ikertzaile anonimo batek, Trend Micro-ko Zero Day Initiative-rekin (ZDI) lankidetzan, bufferraren gainezkatze erako ahultasun hauen berri eman dute. Horiek baliatuz erasotzaile batek informazio heda lezake, urrunetik kodea exekutatu edo aplikazioaren funtzionamendu okerra eragin.

Konponbidea:

- 1.00.89 bertsiora eguneratzea

Xehetasuna:

- Pilan edo memoria dinamikoan (heap) proiektuko fitxategietako datuak kopiatu baino lehen sarrera parametroen baliozkotze okerrak ahalbidetu egiten du bufferrak gainezka egitea. Erasotzaile batek bereziki diseinatutako proiektu fitxategiak prozesatu litzake urruneko kodea exekutatzeko. Ahultasun horietarako CVE-2019-10947 eta CVE-2019-10951 identifikatzaileak erreserbatu dira.
- Proiektuko fitxategietako datuak kopiatu baino lehen sarrera parametroen baliozkotze okerrak erasotzaile bati ahalbidetuko lioke mugaz kanpoko irakurketa, informazioa hedatzea lortuz. Ahultasun horretarako CVE-2019-10949 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Zikloaren denboraren manipulazio erako ahultasuna PLC-n hainbat fabrikatzailetan

Argitalpen data: 2019/04/17

Garrantzia: Handia

Kaltetutako baliabideak:

- ABB 1SAP120600R0071 PM554-TP-ETH
- Phoenix Contact 2700974 ILC 151 ETH
- Schneider Modicon M221
- Siemens
    - 6ES7211-1AE40-0XB0 Simatic S7-1211
    - 6ES7314-6EH04-0AB0 Simatic S7-314
    - 6ED1052-1CC01-0BA8 Logo! 8
- WAGO
    - 750-889 KNX IP kontrolatzailea
    - 750-8100 PFC100 kontrolatzailea
    - 750-880 ETH kontrolatzailea

- 750-831 BACnet/IP kontrolatzailea

Azalpena:

Matthias Niedermaier (Hochschule Augsburg), Jan-Ole Malchow (Freie Universita¨t Berlin) eta Florian Fischer (Hochschule Augsburg) segurtasun ikertzaileek baliabideen kontrolik gabeko kontsumo erako ahultasun baten berri eman dute. Hori baliatuz erasotzaile batek zerbitzuaren ukapen egoera eragin lezake kaltetutako gailuan.

Konponbidea:

Fabrikatzaile bakoitzak konponbide ezberdinak eskaini ditu ahultasun horretarako:

- ABB: ahultasuna ez du halakotzat jo. Aldiz, arazoa PLCren kontrolatzailearen konfigurazio oker bati lotuta dagoela dio, fabrikan modu lehenetsian konfiguratu zena. Konfigurazio oker hori ondokoa ezarriz konpon daiteke: egitekoaren lehentasunaren konbinazio egokia, egitekoaren beraren ziklo denbora eta zaintzaren konfigurazioa (watchdog). Informazio gehiago izateko fabrikatzaileak aholkatzen du Onboard Ethernet Handling in CPU Firmware kapitulua irakurtzea.
- Phoenix Contact: ahultasuna arazo ezaguna dela dio, produktu zaharren kasuan konpondu ez dena. Segurtasunarekin zerikusia duten funtzionaltasunetan ahultasunek izango luketen eragina arintzeko neurriak badauzkate une honetan merkatuan dituzten produktuek. Informazio gehiagorako, irakurri konpainiak argitaratutako oharra.
- Schneider Electric: ahultasun hau konpontzeko zuzenketak Modicon M221ren firmwarearen v1.10.0.0 bertsioan aurkitzen dira, eta EcoStruxure Machine Expert - Basic softwarearen kasuan v1.0 bertsioan. Beste aukera bat da Schneider Electric-en softwarearen eguneraketa tresna exekutatzea, EcoStruxure Machine Expert - Basic-en 1.0 bertsioa deskargatu eta instalatzeko. Konpainiak segurtasun ohar bat argitaratu du (SEVD-2019-045-01).
- Siemens: aurkeztu zaion ahultasunari buruzko txostenean jasotako emaitzak ikertu eta baloratu ditu, eta ondorioztatu du txosten horretan ez dela frogatzen bere PLCetarako ahultasun baliagarri bat dagoenik.
- WAGO: bere bezeroei aholkatzen diete kaltetutako gailuak sare itxietan erabiltzea edo beren komunikazioak suebaki batekin babestea, baimendu gabeko sarbideak eragozteko. Gomendatutako beste neurri aringarri bat da sareko trafikoa mugatzea kommutazio abiaduraren mugaren funtzioaren bidez, aplikazioak dituen beharren arabera.

Xehetasuna:

- Kaltetutako gailuek zerbitzuaren ukapen egoera eragiten duten erasoak jasan ditzakete, parte diren sarea paketeekin gainezkatuz. Sareak paketeen karga handi bat izateak kaltetutako gailuaren CPUaren energia kontsumi dezake, eta horrela konfiguratutako ziklo denbora manipulatua izan daiteke. Ondorioz, bere funtzionamendua kaltetu egin daiteke. Ahultasun horretarako CVE-2019-10953 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Schneider Electric, Siemens, Ahultasuna

---

Hainbat ahultasun CODESYS produktuetan

Argitalpen data: 2019/04/22

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Ondoren aipatzen diren CODESYS V3 produktuen aldaera guztiak daude ahultasunek kaltetuta, V3.5.14.20 bertsioa baino lehenagokoren bat erabiltzen badute eta CmpGateway osagaia badute, zeinahi delarik haien CPU edo Sistema eragile mota:

- BeagleBonerako CODESYS Control
- emPC-A/iMX6rako CODESYS Control
- IOT2000erako CODESYS Control
- Linuxerako CODESYS Control
- PFC100erako CODESYS Control
- PFC200erako CODESYS Control
- Raspberry Pi-rako CODESYS Control
- CODESYS Control V3 Runtime System Toolkit
- CODESYS Gateway V3
- CODESYS V3 Development System

Azalpena:

Cirosec GmbH-ko Martin Hartmann segurtasun ikertzaileak bi ahultasunen berri eman du. Horietako bat kritikoa da, kontrolatu gabeko balio aleatorio eta egiaztatu gabeko ezaugarriaren esleipen erakoa. Bestea kritikotasun altukoa da, memoriaren esleipen erakoa. Biak balia daitezke urrunetik. Erasotzaile batek ahultasun horiek arrakastaz baliatuz gero, zerbitzuaren ukapen egoerak eta komunikazioetan etenak eragin litzake.

Konponbidea:

Fabrikatzaileak ahultasun horiek arintzen dituen software bertsio berri bat argitaratu du (V3.5.14.20).

Xehetasuna:

- Kontrolatu gabeko balio aleatorioen esleipen erako ahultasun kritikoa: CODESYS Gateway-k ez du balio aleatorio egokirik erabiltzen komunikazio kanala identifikatzeko eta modu ez-nahikoan egiaztatzen du kanalaren ezaugarria. Ahultasun hau arrakastaz baliatuz gero urruneko erasotzaile batek dauden komunikazio kanalak itxi litzake. Era berean, kanal bat komunikazio zifratu batekin babestuta ez bazegoen, urruneko erasotzaile batek PLC bati bereziki diseinatutako paketeak bidal liezazkioke, aurrez ezarrita dagoen erabiltzaile saio baten barnean. Ahultasun horretarako CVE-2019-9010 identifikatzailea erreserbatu da.
- Kontrolatu gabeko memoriaren esleipen erako kritikotasun altuko ahultasuna: urruneko erasotzaile batek bereziki diseinatutako eskaerak bidal litzake eta horrela kontrolatu gabeko memoriaren esleipenak egin, kaltetutako CODESYS produktuetan. Ahultasun hori arrakastaz baliatuz gero zerbitzuaren ukapen egoerak eragingo lirateke. Ahultasun horretarako CVE-2019-9012 identifikatzailea erreserbatu da.

Etiketak: Komunikazioak, Ahultasuna

Hainbat ahultasun Fujifilm-en FCR Capsula

X/Carbon X-en

Argitalpen data: 2019/04/24

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- CR-IR 357 FCR Carbon X
- CR-IR 357 FCR XC-2
- CR-IR 357 FCR Capsula X

Azalpena:

Scip AGko Marc Ruef eta Rocco Gagliardi ikertzaileak kontrolik gabeko baliabideen kontsumo erako eta sarbideen kontrol desegoki erako hainbat ahultasunen berri eman dute, Fujifilm-en FCR Capsula X/Carbon X gailuei eragiten dietenak. Ahultasun horiek arrakastaz baliatuz gero urruneko erasotzaile batek zerbitzuaren ukapen egoera eragin lezake edo gailura baimenik gabeko sarbidea eskuratuz, eta kode arbitrarioa exekutatzea ere lortuz.

Konponbidea:

- Fujifilm-ek aholkatzen du sistema "Secure Host" funtzionaltasunarekin konfiguratzea. Konfigurazio horrekin gailuak ez ikusiarena egiten dio Fujifilmen irudien eskuratze kontsolaren IP helbidekoa ez den sare trafiko guztiari. Nolanahi ere, konfigurazio horrek eragotzi egiten du irudiak eskuratzeko kontsola batek baino gehiagok CR-IR 357 irakurketa unitatea partekatzea.Irakurketa unitatea partekatuta ez badago, erabiltzaileak harremanetan jarri behar dira Fujifilmekin "Secure Host" funtzionaltasuna gaitzea eskatzeko. Irakurketa unitatea partekatuta badago, erabiltzaileak Fujifilmekin jarri behar dira harremanetan eskuragarri dauden aukerak aztertzeko.
- Modu osagarrian, Fujifilmek aholkatzen du segurtasun kontrol konpentsatzaileak aplikatzea erabiltzailearen sarean. Neurriak hartu behar dira ziurtatzeko baimena duten gailu eta langileek soilik daukatela sarbidea sarera. Sare publikoak edo gonbidatuak segmentatuta egon behar dira, edo bestela erabiltzaileek VLAN erabili behar dute trafiko publikoa sare pribatutik bereizteko. Fujifilmek kontrol administratiboak eta teknikoak ere ezartzea gomendatzen du.

Xehetasuna:

- Gailuak TCP paketeen gainezkatzea jasaten duenean eskuz berrabiatzea beharrezkoa da, eta horrek zerbitzuaren ukapen egoera eragiten du. Ahultasun horretarako CVE-2019-10948 identifikatzailea erabili da.
- Gailuak telnet zerbitzu ez-seguruak eskaintzen ditu, eta horiek ez dute autentifikazio beharrik. Ahultasun hori arrakastaz baliatuz gero, urruneko erasotzaile batek azpiko sistema eragilera sarbidea lor lezake. Ahultasun horretarako CVE-2019-10950 identifikatzailea erabili da.

Etiketak: Ahultasuna

Hainbat ahultasun Phoenix Contact-en AXC F 2152-n

Argitalpen data: 2019/04/24

Garrantzia: Handia

Kaltetutako baliabideak:

- AXC F 2152 eta Starterkit AXC F 2152, firmwarearen 1.x bertsioa

Azalpena:

Firmalyzer SPRLko Zahra Khani ikertzaileak eta OPC Foundation-ek Phoenix Contact-en AXC F 2152 gailuei eragiten dieten hainbat ahultasunen berri eman dute. Ahultasun horiek arrakastaz baliatuz gero gailuaren konfidentzialtasunari, integritateari edo eskuragarritasunari eragitea legoke.

Konponbidea:

- Ahultasun horiek konpontzeko, Phoenix Contact-ek gomendatzen du gailuak Firmwarearen eta PLCnext Engineer-en 2019.0 LTS edo geroagoko bertsioetara eguneratzea.
- Modu osagarrian, CVE-2018-7559 identifikatzailea duen ahultasunaren kasuan, Phoenix Contact-ek gomendatzen du OPC zerbitzarien konfigurazioan Basic128Rsa15 segurtasun politika desgaitzea eta beti erabiltzea Basic256 edo goragokoa.

Xehetasuna:

- AXC F 2152 gailuaren 1.x firmware bertsioak hirugarren parteen software bertsio zahar ahulak erabiltzen ditu. Ahultasun horien identifikatzaileen zerrenda honakoa da: CVE-2016-6301, CVE-2017-11108, CVE-2017-11541, CVE-2017-11542, CVE-2017-11543, CVE-2017-15906, CVE-2016-1247, CVE-2018-1000117, CVE-2017-9233, CVE-2017-3735, CVE-2017-3731, CVE-2017-3738, CVE-2017-3737, CVE-2018-0737, CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843, CVE-2018-1000122, CVE-2018-1000301, CVE-2017-8817, CVE-2018-1000120, CVE-2018-1000121, CVE-2016-9952, CVE-2016-9953, CVE-2017-1000101, CVE-2017-8816, CVE-2017-1000254, CVE-2017-1000100, CVE-2017-1000257, CVE-2018-1000005, CVE-2016-7141, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2016-7444, CVE-2017-9023, CVE-2018-5388, CVE-2017-9022, CVE-2017-11185, CVE-2015-9251, CVE-2016-7103.
- Urruneko erasotzaile batek man in the middle bat egin lezake eta zerbitzuaren ukapen egoera eragin PC WORX Engineer-en fuzzing-en protokoloan, PLCren zerbitzua geldituz. Zerbitzua berrezartzeko gailua berrabiarazi behar da edo eskuz berrezarri Linuxen kontsolaren bidez. Ahultasun horretarako CVE-2019-10997 identifikatzailea erreserbatu da.
- Gailura sarbide fisikoa lukeen erasotzaile batek SD txartela atera lezake eta bere datuak manipulatu. Horrela gailuaren autentifikazioa saihets lezake. Ahultasun horretarako CVE-2019-10998 identifikatzailea erreserbatu da.
- Urruneko erasotzaile batek OPC zerbitzariaren Basic128Rsa15 segurtasun politikak duen ahultasun bat balia lezake, bereziki diseinatutako erabiltzaileen identifikazio tokenak bidaliz. Horrela erasotzaileak Basic256Sha256 bezalako politika sendoagoen pasahitzak deszifra litzake.Ahultasun horretarako CVE-2018-7559 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Asmo gaiztoko birbideratzailea Rockwell Automation produktuetan

Argitalpen data: 2019/04/24

Garrantzia: Handia

Kaltetutako baliabideak:

- MicroLogix 1400 controllers:
  - A seriea, bertsio guztiak
  - B seriea, 15.002 bertsioa eta lehenagokoak
- MicroLogix 1100 controllers, 14.00 bertsioa eta lehenagokoak
- CompactLogix 5370 L1 eta L2 controllers, 30.014 bertsioa eta lehenagokoak
- CompactLogix GuardLogix controllers-dun CompactLogix 5370 L3, 30.014 bertsioa eta lehenagokoak

Azalpena:

Josiah Bryan eta Geancarlo Palavicini ikertzaileek asmo gaiztoko birbideratzaile erako ahultasun honen berri eman dute, Rockwell Automation-en hainbat produkturi eragiten diena. Ahultasun hau arrakastaz baliatuz gero, autentifikaziorik gabeko erasotzaile batek erabiltzailea birbidal lezake asmo gaiztoko webgune batera.

Konponbidea:

Rockwell Automation-ek ondoko konponbideak eskaintzen ditu kaltetutako ekipoetarako:

- MicroLogix 1400 controllers A seriearen kasuan, gailuan HTTP parametroa desgaitzea.
- MicroLogix 1400 controllers B seriearen kasuan, FRN 15.003 edo ondorenekoa aplikatzea.
- MicroLogix 1100 controllers-en kasuan, FRN 15.000 edo ondorenekoa aplikatzea.
- CompactLogix 5370 L1 controllers, L2 controllers eta L3 controllers-en kasuan, 31.011 edo ondoreneko bertsioa aplikatzea.

Xehetasuna:

Autentifikaziorik gabeko urruneko erasotzaile batek asmo gaiztoko lotura bat sar lezake, erabiltzaileak asmo gaiztoko webgune batera birbidaltzeko. Horrela erasotzaileak malwarea deskargatu edo exekutatu lezake erabiltzailearen makinan. Ahultasun horretarako CVE-2019-10955 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna