2020ko Apirilaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Bufferraren gainezkatzea Hirschmann-en hainbat produktutan

Argitalpen data: 2020/04/01

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- 07.0.02 eta lehenagoko bertsioetan HiOS erabiltzen duten RSP, RSPE, RSPS, RSPL, MSP, EES, EES, EESX, GRS, OS, RED gailuak.
- 03.2.00 eta lehenagoko bertsioetan HiSecOS erabiltzen duten EAGLE20/30 gailuak.

Azalpena:

GAI NetConsult GmbH-eko Sebastian Krause eta Toralf Gimpel ikertzaileek larritasun kritikoko ahultasun baten berri eman dute, Hirschmann-en hainbat produkturi eragiten diena. Autentifikatu gabeko urruneko erasotzaile batek bufferraren gainezkatzea eragin lezake eta gailua arriskuan jarri.

Konponbidea:

- HiOS erabiltzen duten produktuak 07.0.03 bertsiora edo berriago batera eguneratzea.
- HiSecOS erabiltzen duten produktuak 03.3.00 bertsiora edo berriago batera eguneratzea.

Xehetasuna:

Ahultasunaren jatorria URLren argumentuen analisi desegoki bat da. Erasotzaile batek ahultasun hori balia lezake HTTP eskaerak bereziki sortuz barne buffer bat gainezkatzeko. Ahultasun horretarako CVE-2020-6994 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Informazioaren ihes erako ahultasuna PEPPERL FUCHSen Tab-Ex 02-n

Argitalpen data: 2020/04/01

Garrantzia: Txikia

Kaltetutako baliabideak:

Tab-Ex 02, 01.03.2020 eta lehenagoko bertsioak.

Azalpena:

ESETeko ikertzaileek larritasun baxuko ahultasun baten berri eman dute, Kr00k izenekoa eta informazioaren ihes erakoa, PEPPERL FUCHS fabrikatzailearen Tab-Ex 02 produktuari eragiten diona.

Konponbidea:

Fabrikatzaileak kaltetutako produkturako eguneraketa bat argitaratzeko asmoa dauka 2020ko maiatzean.

Xehetasuna:

Aurkitutako ahultasunak Broadcom edo Cypress chipset-ak erabiltzen dituzten gailuetarako wifiren trafiko zifratuari eragiten dio. Erasotzaile batek WPA2-Personal/Enterprise trafikoaren parte bat deszifra lezake, AP(Access Point)/bezero bati behartuz all-zero zifratuaren gako bat erabiltzen hastera. Ahultasun horretarako CVE-2019-15126 identifikatzailea erabili da.

Etiketak: Komunikazioak, Ahultasuna

Murriztutako mahaigaineko ingurunearen ihes erako ahultasuna Becton, Dickinson and Company-ren (BD) produktuetan

Argitalpen data: 2020/04/01

Garrantzia: Ertaina

Kaltetutako baliabideak:

- Pyxis MedStation ES System, 1.6.1 bertsioa;
- Pyxis Anesthesia (PAS) ES System, 1.6.1 bertsioa.

Azalpena:

BDren ekipoak babes mekanismoaren akats erako ahultasun bat aurkitu du BDren hainbat produktutan. Hori baliatuz, sarbide fisikoa lukeen erasotzaile batek gailuko datu sentikorrak ikusi edota alda litzake.

Konponbidea:

BDk ez du argitaratu inolako eguneraketarik ahultasun hori konpontzeko, baina bezeroei ondoko neurriak ezartzea aholkatzen die:

- Pyxis Medstation ES eta Anesthesia (PAS) ES sistemetarako sarbide fisikoa soilik erabiltzaile baimenduei ematea;
- eragindako sistemak isolatzea eta konfiantzako sistemetara soilik konektatzea;
- sistemen ustekabeko berrabiatzeak zaintzea eta ikertzea, IT sailek eskainitako sareak zaintzeko tresnak erabiliz.

Xehetasuna:

Murriztutako mahaigaineko ingurunearen ihes erako ahultasuna baliatuz, kaltetutako gailuek kiosko moduaren funtzionaltasunean dutena, erasotzaile batek datu sentikorretara sarbidea lor lezake bereziki diseinatutako sarreren bidez. Ahultasun horretarako CVE-2020-10598 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun ABBren produktuetan

Argitalpen data: 2020/04/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- System 800xA Base, 6.1 eta lehenagoko bertsioak;
- System 800xA Information Manager:
  - 5.1 bertsioa;
  - 6.0.0 bertsioa, 6.0.3.2 bertsiora bitartean;
  - 6.1 bertsioa.
- TG/S 3.2 Telephone Gateway, Analogue, MDRC;
- 6186/11 Telefon-Gateway, Analog (Busch-Jaeger brand);
- OPC Server para AC800M, 6.0 eta lehenagoko bertsioak;
- Control Builder MProfessional, 6.1 eta lehenagoko bertsioak;
- AC800Merako MMSServer, 6.1 eta lehenagoko bertsioak;
- SoftControl-erako Base Software, 6.1 eta lehenagoko bertsioak.

Azalpena:

Applied Risk-eko William Knowles ikertzaileak eta Maxim Risk ikertzaileak ABBren hainbat produkturi eragiten dieten 8 ahultasunen berri eman dute, bi larritasun kritikokoak, hiru altukoak eta hiru ertainekoak. Urruneko sarbidea lukeen erasotzaile batek gailua geldi lezake, modu arbitrarioan kodea exekutatu, gailuaren kontrola hartu eta pribilegioen eskalatzea egin.

Konponbidea:

- System 800xA Base ondoko ekintzetako edozeinekin konpon daiteke:
  - eskuragarri dagoen azken bertsiora eguneratzea, 6.1;
  - 6.0.3 LTS bertsiora eguneratzea, 6.0.33ren ondoren.
- TG/S 3.2 Telephone Gateway, Analogue, MDR y 6186/11 Telefon-Gateway, Analog (Busch-Jaeger brand):
  - Gailuak sare seguruetan soilik konfiguratzea.
- 6.0.3 LTS bertsiora eguneratzea, 6.0.3.3ren ondoren:
  - System 800xA Information Manager,
  - AC800Merako MMSServer,
  - AC800Merako OPC Server,
  - Control Builder MProfessional,
  - SoftControl-erako Base Software.

Xehetasuna:

Ondoren zehazten dira larritasun kritiko edo altuko ahultasunak:

- Windowseko erregistrorako sarbide kontrolaren konfigurazioak pribilegio gutxiko erabiltzaileei ahalbidetzen die sistemaren funtzioek erabilitako edukia irakurri eta aldatzea. Erasotzaile autentifikatu batek sistema ezberdinen funtzionamendu okerra eragin

lezake. Ahultasun horretarako CVE-2020-8474 identifikatzailea erreserbatu da.
- Berehalako mezularitzaren (IM) zerbitzariak duen osagai ahul bat baliatuz, erasotzaile batek kode arbitrarioa exekuta lezake biktimaren ekipoan. Ahultasun hori arrakastaz baliatzeko, beharrezkoa da erabiltzailea konbentzitzea asmo gaiztoko webgune batera sar dadin. Ahultasun horretarako CVE-2020-8477 identifikatzailea erreserbatu da.
- Produktuaren web zerbitzari integratuan URL jakin batera sartzean, asmo gaiztoko erabiltzaile batek aplikazioaren azken puntu ezberdinetara sarbidea lor lezake autentifikatu behar izan gabe, sarbideko kontrol arauak (ACL) saihestuz. Erasotzaile batek informazio konfidentziala eskuratu lezake edo pribilegioak eskalatzea lortu. Ahultasun horretarako CVE-2019-19104 identifikatzailea erreserbatu da.
- Aplikazioak ez ditu erabiltzen sarbidearen kontrolerako arau egokiak (ACL). Erasotzaile batek informazioa eskura lezake edo sistemaren konfigurazioak aldatu. Ahultasun horretarako CVE-2019-19106 identifikatzailea erreserbatu da.
- ABB Sistemaren 800xA Base-ren funtzioetako batean dagoen ahultasuna arrakastaz baliatuz gero, erasotzaile batek pribilegioen eskalatzea egin lezake, kode arbitrarioa exekutatu eta ingeniaritzako hainbat funtziori eragin, eta horrek aplikazio uztelak eragingo lituzke. Ahultasun horretarako CVE-2020-8473 identifikatzailea erabili da.

Gainerako ahultasunei honako identifikatzaileak esleitu zaizkie: CVE-2019-19105, CVE-2019-19107 eta CVE-2020-8472.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Hainbat ahultasun B&Rren Automation Studio-n

Argitalpen data: 2020/04/03

Garrantzia: Altua

Kaltetutako baliabideak:

Automation Studio, honako bertsioak:

- 4.0.x;
- 4.1.x;
- 4.2.x;
- 4.3.11SP eta lehenagokoak;
- 4.4.9SP eta lehenagokoak;
- 4.5.4SP eta lehenagokoak;
- 4.6.3SP eta lehenagokoak;
- 4.7.2 eta lehenagokoak;
- 4.8.1 eta lehenagokoak.

Azalpena:

Nadav Erez ikertzaileak hiru ahultasunen berri eman du: pribilegioen kudeaketa okerra, murriztutako direktorio baterako bidearen izenaren murrizpen okerra, eta beharrezkoa den zifratuaren urrats falta. Horiek baliatuz erasotzaile batek fitxategiak ezaba litzake arbitrarioki, fitxategi arbitrarioak bilatu edo idazketa eragiketa arbitrarioak egin Automation Studio produktuan.

Konponbidea:

Azken bertsiora eguneratzea.

Xehetasuna:

- B&R Automation Studio-ren eguneraketa zerbitzuan pribilegioen eskalatzea baliatuz, erasotzaile autentifikatu batek fitxategi arbitrarioak ezaba litzake agerian jarritako interfaze baten bidez. Ahultasun horretarako CVE-2019-19100 identifikatzailea erreserbatu da.
- Eguneraketa zerbitzuan segurtasunik gabeko komunikazio bat eta TLS baliozkotze osagabe bat baliatuz, autentifikatu gabeko erasotzaile batek MITM erasoak egin litzake B&R eguneraketa zerbitzuaren bidez. Ahultasun horretarako CVE-2019-19101 identifikatzailea erreserbatu da.
- SharpZipLib direktorioak duen ahultasun transbertsal bat B&Rren eguneraketa zerbitzuan erabiltzen da. Hori baliatuz autentifikatu gabeko erasotzaile batek hainbat direktorio lokaletan idatz lezake. Ahultasun horretarako CVE-2019-19102 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Advantech WebAccess/NMS-n

Argitalpen data: 2020/04/08

Garrantzia: Kritikoa

Kaltetutako baliabideak:

WebAccess/NMS, 3.0.2 baino lehenagoko bertsioak.

Azalpena:

9sg-ko rgod-ek, Trend Micro-ko Zero Day Initiative-rekin lankidetzan, 8 ahultasunen berri eman du, horietatik 2 larritasun kritikokoak, 5 altukoak eta 1 ertainekoa. Ahultasun motak honakoak dira: asmo gaiztokoak izan litezkeen fitxategien murrizpenik gabeko igoera, SQL injekzioa, bideetara sarbide erlatibo ez kontrolatua (*relative path traversal*), funtzio kritikorako autentifikazio falta, XXErako (*XML eXternal Entities*) erreferentzien murrizpen desegokia eta Sistema Eragilearen komandoen injekzioa..

Konponbidea:

Kaltetutako produktua 3.0.2 bertsiora eguneratzea..

Xehetasuna:

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

- asmo gaiztokoak izan litezkeen fitxategiak igotzea eta exekutatzea;

- informazio sentikorrera sarbidea lortzea;
- aplikazioaren kontroletik kanpoko fitxategiak ezabatzea edo aldatzea;
- administratzaile profilak sortzea;
- sistemako komandoak urrunetik exekutatzea

Ahultasun horietarako honako identifikatzaileak erreserbatu dira: CVE-2020-10617, CVE-2020-10623, CVE-2020-10619, CVE-2020-10631, CVE-2020-10625, CVE-2020-10629 eta CVE-2020-10603..

Etiketak: Eguneraketa, Azpiegitura kritikoak, Ahultasuna

Ahultasuna Fuji Electric V-Server Lite-n

Argitalpen data: 2020/04/08

Garrantzia: Altua

Kaltetutako baliabideak:

V-Server Lite, 4.0.9.0 baino lehenagoko bertsio guztiak..

Azalpena:

Memoria dinamikoan (heap) oinarritutako bufferraren gainezkatze erako ahultasun bat baliatuz, erasotzaile batek urrunetik kodea exekuta lezake.

Konponbidea:

4.0.9.0 bertsiora eguneratzea..

Xehetasuna:

Datuen irakurketara esleitutako bufferra txikiegia da VPR fixategiak aztertzean. Hori baliatuz urruneko erasotzaile batek pribilegioak eskalatu litzake kodea urrunetik exekutatzeko. Ahultasun horretarako CVE-2020-10646 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna, Azpiegitura kritikoak

Hainbat ahultasun Universal Robots-en produktuetan

Argitalpen data: 2020/04/08

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- UR10,
- UR5,
- UR 3,
- Universal Robots Robot Controllers CB 2, CB3 eta e-series.

Azalpena:

Alias Robotics-eko ikertzaileek, ikertzaile independenteekin lankidetzan, 86 ahultasun aurkitu dituzte, horietako 29 larritasun kritikokoak, 37 altukoak, 19 ertainekoak eta 1 baxukoa.

Aipatutako ahultasunen artetik nabarmentzekoak dira bi larritasun kritikokoak (CVE-2020-10264 eta CVE-2020-10265) eta beste bi altukoak (CVE-2020-10266 eta CVE-2020-10267).

Konponbidea:

Oraingoz ez dago ahultasun horiek konpontzen dituen eguneraketarik.

CVE-2020-10266 identifikatzailea duen ahultasunaren kasuan, arintze neurri modura gomendatzen da UR+ plataformako osagaiak digitalki sinatzea, eta sinadura baliozkotzea instalazio prozesuan zehar.

CVE-2020-10267 identifikatzailea duen ahultasunaren kasuan, arintze neurri modura zifratuaren eta sinaduraren konbinaketa bat erabiltzea gomendatzen da instalatutako jabetza intelektuala babesteko. Fitxategi horiek dauden fitxategi sistemak irakurketa baimenak soilik dituela ziurtatzea, salbu eta baimendutako aldaketetarako.

Ohartarazpen hau eguneratuko da eguneraketa berriak argitaratzen direnean.

Xehetasuna:

Ahultasunak baliatuz erasotzaile batek ondoko ekintzak egin litzake:

- Informazio sentikorra ezagutzera ematea.
- Sistemaren urruneko kontrola eskuratzea.
- Sisteman aldaketak egitea.
- Kodearen urruneko exekuzioa.
- Zerbitzuaren ukapen egoera eragitea.
- Sistema ustekabean ixtea.

Etiketak: Ahultasuna

Baimenen esleipen okerra Rockwell Automation-en RSLinx Classic-en

Argitalpen data: 2020/04/13

Garrantzia: Altua

Kaltetutako baliabideak:

RSLinx Classic, 4.11.00 bertsioa eta lehenagokoak.

Azalpena:

Applied Risk-eko ikertzaileek larritasun altuko ahultasun baten berri eman zioten fabrikatzaileari, baliabide kritikoetarako baimenen esleipen oker erakoa.

Konponbidea:

3.60tik 4.11ra bitarteko bertsioen kasuan 1091155 partxea aplikatzea, baina fabrikatzaileak gomendatzen du kaltetutako produktua bertsiorik berrienera eguneratzea.

Xehetasuna:

Autentifikatutako erasotzaile lokal batek ahultasun hori balia lezake erregistroko gako bat aldatzeko, eta horrek asmo gaiztoko kodea exekutatzea eragin lezake, sistemaren pribilegioak erabiliz RSLinx Classic irekitzean. Ahultasun horretarako CVE-2020-10642 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Ahultasuna

Siemens-en 2020ko apirileko segurtasun buletina

Argitalpen data: 2020/04/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Climatix POL908 (BACnet/IP module), bertsio guztiak;
- Climatix POL909 (AWM module), bertsio guztiak;
- IE/PB-Link V3, bertsio guztiak;
- KTK ATE530S, bertsio guztiak;
- RUGGEDCOM RM1224, 6.1 baino lehenagoko bertsio guztiak;
- RUGGEDCOM ROX II, 2.13.3 baino lehenagoko bertsio guztiak;
- SCALANCE:
  - M-800 family, 6.1 baino lehenagoko bertsio guztiak;
  - S615, 6.1 baino lehenagoko bertsio guztiak;
  - SC-600, 2.0 baino lehenagoko bertsio guztiak;
  - W1700 IEEE 802.11ac, 2.0 baino lehenagoko bertsio guztiak;
  - W700 IEEE 802.11a/b/g/n, 6.4 baino lehenagoko bertsio guztiak;
  - X-200 switch family (SIPLUSNET aldaerak barne), bertsio guztiak;
  - X-200IRT switch family (SIPLUSNET aldaerak barne), bertsio guztiak;
  - X-300 switch family (X408 eta SIPLUS NET aldaerak barne), bertsio guztiak.
- SIDOOR ATD430W, ATE530S COATED eta ATE531S, bertsio guztiak;
- SIMATIC CP 1242-7, 3.2 baino lehenagoko bertsio guztiak;
- SIMATIC CP 1243-1 (SIPLUS NET aldaerak barne), 3.2 baino lehenagoko bertsio guztiak;
- SIMATIC CP 1243-7 LTE EU, 3.2 baino lehenagoko bertsio guztiak;
- SIMATIC CP 1243-7 LTE US, 3.2 baino lehenagoko bertsio guztiak;
- SIMATIC CP 1243-8 IRC, 3.2 baino lehenagoko bertsio guztiak;
- SIMATIC CP 1542SP-1 IRC (SIPLUS NET aldaerak barne), 2.1 baino lehenagoko bertsio guztiak;
- SIMATIC CP 1542SP-1, 2.1 baino lehenagoko bertsio guztiak;
- SIMATIC CP 1543-1 (SIPLUS NET aldaerak barne), 2.2 baino lehenagoko bertsio guztiak;
- SIMATIC CP 1543SP-1 (SIPLUS NET aldaerak barne), 2.1 baino lehenagoko bertsio guztiak;
- SIMATIC CP 443-1 (SIPLUS NET aldaerak barne), bertsio guztiak;
- SIMATIC CP 443-1 Advanced (SIPLUS NET aldaerak barne), bertsio guztiak;
- SIMATIC ET 200SP Interfacemodul IM 155-6 MF HF, bertsio guztiak;
- SIMATIC ET 200SP Open Controller CPU 1515SP PC (SIPLUS aldaerak barne), 2.0 baino lehenagoko bertsio guztiak;
- SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (SIPLUS aldaerak barne), 2.0 baino lehenagoko bertsio guztiak;
- SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (SIPLUS aldaerak barne), 2.08 baino lehenagoko BIOS bertsio guztiak;
- SIMATIC ET200MP IM155-5 PN HF (SIPLUS aldaerak barne), 4.2 eta lehenagoko bertsioak;
- SIMATIC ET200SP IM155-6 PN HA (SIPLUS aldaerak barne), bertsio guztiak;
- SIMATIC ET200SP IM155-6 PN HF (SIPLUS aldaerak barne), 4.2 eta lehenagoko bertsioak;
- SIMATIC ET200SP IM155-6 PN/2 HF (SIPLUS aldaerak barne), 4.2 eta lehenagoko bertsioak;
- SIMATIC ET200SP IM155-6 PN/3 HF (SIPLUS aldaerak barne), 4.2 eta lehenagoko bertsioak;
- SIMATIC Field PG M4, PG M5 eta PG M6, bertsio guztiak;
- SIMATIC IPC127E, 27.01.04 baino lehenagoko BIOS bertsio guztiak;
- SIMATIC IPC427C, bertsio guztiak;
- SIMATIC IPC427D (SIPLUS aldaerak barne), bertsio guztiak;
- SIMATIC IPC427E (SIPLUS aldaerak barne), bertsio guztiak;
- SIMATIC IPC477C, bertsio guztiak;
- SIMATIC IPC477D, bertsio guztiak;
- SIMATIC IPC477E PRO, bertsio guztiak;
- SIMATIC IPC477E, bertsio guztiak;
- SIMATIC IPC527G, bertsio guztiak;
- SIMATIC IPC547E, bertsio guztiak;
- SIMATIC IPC547G, bertsio guztiak;
- SIMATIC IPC627C, bertsio guztiak;
- SIMATIC IPC627D, bertsio guztiak;
- SIMATIC IPC627E, 25.02.05 baino lehenagoko BIOS bertsio guztiak;

- SIMATIC IPC647C, bertsio guztiak;
- SIMATIC IPC647D, bertsio guztiak;
- SIMATIC IPC647E, 25.02.05 baino lehenagoko BIOS bertsio guztiak;
- SIMATIC IPC677C, bertsio guztiak;
- SIMATIC IPC677D, bertsio guztiak;
- SIMATIC IPC677E, 25.02.05 baino lehenagoko BIOS bertsio guztiak;
- SIMATIC IPC827C, bertsio guztiak;
- SIMATIC IPC827D, bertsio guztiak;
- SIMATIC IPC827E, bertsio guztiak;
- SIMATIC IPC847C, bertsio guztiak;
- SIMATIC IPC847D, bertsio guztiak;
- SIMATIC IPC847E, 25.02.05 baino lehenagoko BIOS bertsio guztiak;
- SIMATIC ITP1000, bertsio guztiak;
- SIMATIC MICRO-DRIVE PDC, bertsio guztiak;
- SIMATIC PN/PN Coupler (SIPLUS NET aldaerak barne), 4.2 eta lehenagoko bertsioak;
- SIMATIC RF180C, bertsio guztiak;
- SIMATIC RF182C, bertsio guztiak;
- SIMATIC RF185C, bertsio guztiak;
- SIMATIC RF186C eta RF186CI, bertsio guztiak;
- SIMATIC RF188C eta RF188CI, bertsio guztiak;
- SIMATIC S7-1500 CPU family (related ET200 CPUs eta SIPLUS aldaerak barne), 2.0 baino lehenagoko bertsio guztiak;
- SIMATIC S7-1500 Software Controller, 2.0 bertsioa baino lehenagoko guztiak;
- SIMATIC S7-1500 CPU family (related ET200 CPUs eta SIPLUS aldaerak barne), bertsio guztiak;
- SIMATIC S7-400 PN/DP V7 eta CPU family behekoak (SIPLUS aldaerak barne), bertsio guztiak;
- SIMATIC S7-410 CPU family (SIPLUS aldaerak barne), bertsio guztiak;
- SIMATIC TDC CP51M1, bertsio guztiak;
- SIMATIC TDC CPU555, bertsio guztiak;
- SIMATIC WinAC RTX (F) 2010, bertsio guztiak;
- SIMOTION P320-4E, bertsio guztiak;
- SIMOTION P320-4S, bertsio guztiak;
- SINAMICS S/G Control Unit w. PROFINET, bertsio guztiak;
- SINEMA Remote Connect Server, >V1.1 eta
- TIM 3V-IE (SIPLUS NET aldaerak barne), 2.8 baino lehenagoko bertsio guztiak;
- TIM 3V-IE Advanced (SIPLUS NET aldaerak barne), 2.8 baino lehenagoko bertsio guztiak;
- TIM 3V-IE DNP3 (SIPLUS NET aldaerak barne), 3.3 baino lehenagoko bertsio guztiak;
- TIM 4R-IE (SIPLUS NET aldaerak barne), 2.8 baino lehenagoko bertsio guztiak;
- TIM 4R-IE DNP3 (SIPLUS NET aldaerak barne), 3.3 baino lehenagoko bertsio guztiak.

Azalpena:

Ohartarazpen honek Siemensen hainbat produkturi eragiten dieten 10 ahultasun jasotzen ditu, horietatik 2 larritasun kritikokoak dira, 6 larritasun altukoak eta 2 larritasun ertainekoak.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak Siemens-en deskarga paneletik eskura daitezke. Eguneraketarik eskuragarri ez daukaten produktuen kasuan Erreferentziak atalean azaltzen diren arintze neurriak ezarri behar dira.

Xehetasuna:

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

- Zerbitzuaren Ukapen egoera (DoS) eragitea;
- gailuaren kontrola eskuratzea;
- pribilegioak eskalatzea;
- informazioa ezagutzera ematea;
- kodearen urruneko exekuzioa.

Ahultasun horietarako honako identifikatzaileak erreserbatu dira: CVE-2019-19301, CVE-2019-10939, CVE-2018-5390, CVE-2018-5391, CVE-2019-0151, CVE-2019-0152, CVE-2019-0169, CVE-2019-19300, CVE-2020-7574 eta CVE-2020-7575.

Etiketak: Eguneraketa, Siemens, Ahultasuna

Hainbat ahultasun Eaton-en HMiSoft VU3-n

Argitalpen data: 2020/04/15

Garrantzia: Altua

Kaltetutako baliabideak:

HMiSoft VU3, 3.00.23 bertsioa eta lehenagokoak.

Azalpena:

Natnael Samson-ek, Trend Micro-ko ZDIrekin lankidetzan, bi ahultasunen berri eman diote CISAri, bat larritasun altukoa eta bestea ertainekoa, pilan oinarritutako bufferraren gainezkatze eta mugaz kanpoko irakurketa erakoak.

Konponbidea:

Eaton-ek kaltetutako produktua fabrikatzeari utzi zion 2018/12/31n, eta beraz gaur egun ez dauka beretzako zerbitzu teknikorik ezta segurtasun zuzenketarik ere. HMiVU ordezkatua izan zen XV100 eta XV300 produktu sortarekin.HMiVUren erabiltzaileei gomendatzen zaie Eaton-ekin harremanetan jartzea laguntza teknikoa edo XV soluziora migratzeko laguntza lortzeko.

Xehetasuna:

- Bereziki diseinatutako sarrera fitxategi batek pilaren (stack) bufferraren gainezkatzea eragin dezake produktu kaltetuak kargatzen duenean. Ahultasun horretarako CVE-2020-10639 identifikatzailea erreserbatu da.
- Bereziki diseinatutako sarrera fitxategi batek mugez kanpoko irakurketa eragin lezake produktu kaltetuak kargatzen duenean. Ahultasun horretarako CVE-2020-10637 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna

Hainbat ahultasun Triangle MicroWorks-en gailuetan

Argitalpen data: 2020/04/15

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- DNP3 Outstation .NET Protocol osagaiak, eta DNP3 Outstation ANSI C liburutegiak, 3.16.00 bertsiotik 3.25.01 bitartean.
- SCADA Data Gateway:
  - 3.02.0697 bertsiotik 4.0.1.22 bertsiora bitartekoak;
  - 2.41.0213 bertsiotik 4.0.1.22 bertsiora bitartekoak.

Azalpena:

Steven Seely eta Chris Anastasio ikertzaileek, Trend Micro-ko ZDIrekin lankidetzan, lau ahultasunen berri eman diote Triangle MicroWorks-i, bi larritasun kritikokoak, beste bat kritikotasun altukoa eta beste bat kritikotasun ertainekoa. Autentifikatu gabeko urruneko erasotzaile batek kodearen exekuzioa eten lezake, kode arbitrarioa exekutatu edo zerbitzuaren ukapen egoera (DoS) sortu.

Konponbidea:

- DNP3 Outstation .NET Protocol eta DNP3 Outstation ANSI C eguneratzea 3.26 bertsiora.
- SCADA Data Gateway 4.0.123 bertsiora eguneratzea.

Xehetasuna:

DNP3 Outstation-ek duen larritasun kritikoko ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek, bereziki diseinatutako mezu bat bidaliz, pilan oinarritutako bufferraren gainezkatzea eragin lezake, ekipoan kodearen exekuzioa eten lezakeena. Ahultasun horretarako CVE-2020-6996 identifikatzailea erreserbatu da.

SCADA Gateway-k duen larritasun kritikoko ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek kode arbitrarioa exekuta lezake, erabiltzaileak emandako datuen baliozkotze falta dela eta. Ahultasun horretarako CVE-2020-10611 identifikatzailea erreserbatu da.

SCADA Data Gateway-k duen larritasun altuko ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake, erabiltzaileak emandako datuen luzeraren baliozkotze falta dela eta. Ahultasun horretarako CVE-2020-10615 identifikatzailea erreserbatu da.

Larritasun ertaineko ahultasunerako CVE-2020-10615 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, SCADA, Ahultasuna

Schneider Electric-en 2020ko apirileko segurtasun buletina

Argitalpen data: 2020/04/15

Garrantzia: Altua

Kaltetutako baliabideak:

- SoMachine, SoMachine Basic eta SoMachine Motion, bertsio guztiak;
- EcoStruxure Machine Expert eta Basic, bertsio guztiak;
- Modicon M100/M200/M218/M221/M241/M251/M258 Logic Controller, bertsio guztiak;
- Vijeo Designer Basic, 1.1 HotFix 15 eta lehenagoko bertsioak;
- Vijeo Designer, 6.9 SP9 eta lehenagoko bertsioak;
- TriStation TS1131, 4.0.0tik 4.9.0 eta 4.10.0 bertsioetaraino, Windows NT, Windows XP eta Windows 7n exekutatzen direnean;
- Tricon, 10.0, 10.1, 10.2.x eta 10.3.x bertsioak;
- Tricon Communications Module, 4351, 4352, 4351A/B eta 4352A/B modeloak.

Azalpena:

Trustwave-ko Seok Min Lim eta Johnny Pan, 307Lab eta Zhejiang University-ko Rongkuan Ma, Shunkai Zhu eta Peng Cheng, nsfocus-eko Yongjun Liu, eta beste ikertzaile independente batek larritasun altu eta ertaineko 8 ahultasunen berri eman diote Schneider Electric-i, era ezberdinetakoak: elementuen neutralizazio desegokia irteeran, datuen egiazkotasunaren baliozkotze ez-nahikoa, datu sentikorren transmisioa zifratu gabe, fidagarria ez den bilaketa bidea, zerbitzuaren ukapena eta *host*-era sarbide desegokia.

Konponbidea:

Fabrikatzailearen ohartarazpen bakoitzean *Remediation / Available Remediations* atalean azaldutako eguneratze eta konfiguratze jarraibideak betetzea.

Xehetasuna:

Ahultasun horiek baliatuko lituzkeen erasotzaile batek honako ekintzak egin litzake:

- asmo gaiztoko kodearen transferentzia kontrolatzailera,
- asmo gaiztoko kodea exekutatzea,
- informazio sentikorraren ihesa,
- kode arbitrarioa exekutatzea,
- informazio konfidentziala lauan bidaltzea,

- zerbitzuaren ukapena (DoS),
- sarbide desegokia host makinara,
- moduluen berrasieratzea sareak trafiko altuko baldintzak dituenean.

Ahultasun horietarako honako identifikatzaileak erreserbatu dira: CVE-2020-7489, CVE-2020-7487, CVE-2020-7488, CVE-2020-7490, CVE-2020-7483, CVE-2020-7484, CVE-2020-7485 eta CVE-2020-7486.

Etiketak: Eguneraketa, Schneider Electric, Ahultasuna

.NET bezeroen komunikazioetan asmo gaiztoko mezuen bidalketa OPC UA-n

Argitalpen data: 2020/04/17

Garrantzia: Altua

Kaltetutako baliabideak:

OPC UA .NET Standard Stack eta Sample Code.

Azalpena:

Steven Seeley eta Chris Anastasio ikertzaileek, Trend Micro-ko ZDIrekin lankidetzan, larritasun altuko ahultasun bat aurkitu dute. Horren ondorioz zerbitzari bat deskonektatu egin liteke mezu okerrak jasotzean.

Konponbidea:

Segurtasun partxea ezartzea edo NuGet paketea 1.4.360.33 bertsiora eguneratzea.

Xehetasuna:

Bereziki diseinatutako mezuak bidaliz OPC UA zerbitzariak deskonektatu litezke. Ahultasun horretarako CVE-2020-8867 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Hainbat ahultasun ABB produktuetan

Argitalpen data: 2020/04/22

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- OPC Server for AC 800M, bertsio guztiak;
- MMS Server for AC 800M, bertsio guztiak;
- Base Software for SoftControl, bertsio guztiak;
- 800xA for DCI, bertsio guztiak;
- 800xA for MOD300, bertsio guztiak;
- 800xA RNRP, bertsio guztiak;
- ABB System 800xA Base, bertsio guztiak;
- 800xA Batch Management, bertsio guztiak;
- 800xA Information Management, bertsio guztiak;
- ABB AbilityTM System 800xA eta erlazionatutako sistemen luzapenak 5.1, 6.0 eta 6.1;
- Compact HMI 5.1, 6.0;
- Control Builder Safe 1.0, 1.1 eta 2.0;
- ABB AbilityTM Symphony® Plus - S Operations, 3.0tik 3.2ra;
- ABB AbilityTM Symphony® Plus - S Engineering, 1.1etik 2.2ra;
- Composer Harmony 5.1, 6.0 eta 6.1;
- Composer Melody, honako bertsioak: Melody Composer 5.3, Melody Composer 6.1 / 6.2 eta SPE for Melody 1.0 SPx (Composer 6.3);
- Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 eta 7.0;
- ABBAbility TM System 800xA / Advant® OCS Control Builder A, 1.3 eta 1.4;
- Advant® OCS AC 100 OPC Server 5.1, 6.0 eta 6.1;
- Composer CTK, CTK 6.1, 6.2;
- AdvaBuild, versiones 3.7 SP1 eta 3.7 SP2;
- OPC Server for MOD300 (non-800xA), 1.4;
- OPC DataLink 2.1, 2.2;
- ABB AbilityTM Knowledge Manager 8.0, 9.0 ,9.1;
- ABB AbilityTM Manufacturing Operations Management 1812 eta 1909;
- ABB Central Licensing System (CLS) System 800xA-n, 5.1, 6.0 eta 6.1 bertsioak;
- ABB Central Licensing System (CLS) Compact HMI-n, 5.1 eta 6.0 bertsioak;
- ABB Central Licensing System (CLS) Control Builder Safe-n, 1.0,1.1 eta 2.0 bertsioak.

Azalpena:

ABBko produktuek dituzten hainbat ahultasunen berri eman da, bi larritasun kritikokoak, sei altukoak eta bost ertainekoak. Horiek baliatuz erasotzaile batek sistemaren kontrol osoa eskura lezake, lizentzien zerbitzarira sarbidea lortu, lizentzien maneiua blokeatu, nodoen sistemari esleitutako lizentziak aldatu, pribilegioak eskalatu, kode arbitrarioa exekutatu, sistemaren nodoa eskuragarri jarri edo sistemaren exekuzio denboran datuak manipulatu.

Konponbidea:

Produktuak laster eguneratuko dira. Bitartean, Erreferentziak atalean jasotzen diren arintze neurriak hartu behar lirateke.

Xehetasunak:

- Babestu gabeko fitxategietan gordetako informazio konfidentziala baliatuz, erasotzaile batek sistemaren kontrol osoa eskura lezake. Larritasun kritikoko ahultasun horretarako CVE-2020-8481 identifikatzailea erreserbatu da.
- XML Kanpoko Entitatearen injekzio erako ahultasun bat baliatuz, erasotzaile batek fitxategi arbitrarioak irakurri edo haiei dei egin liezaieke lizentzien zerbitzaritik edota saretik, edo lizentziaren maneiua blokea lezake. Larritasun kritikoko ahultasun horretarako CVE-2020-8479 identifikatzailea erreserbatu da.
- Fitxategien baimen desegokien ahultasun bat baliatuz, erasotzaile batek lizentzien maneiua blokea lezake, pribilegioak eskalatu edo kode arbitrarioa exekutatu. Larritasun altuko ahultasun horretarako CVE-2020-8471 identifikatzailea erreserbatu da.
- Zerbitzuaren ukapen erako ahultasun bat baliatuz erasotzaile batek lizentziaren maneiua blokea lezake. Larritasun ertaineko ahultasun honetarako CVE-2020-8475 identifikatzailea erreserbatu da.
- Pribilegioen eskalatze erako ahultasun bat baliatuz erasotzaile batek nodoen sistemari esleitutako lizentziak alda litzake. Larritasun ertaineko ahultasun honetarako CVE-2020-8476 identifikatzailea erreserbatu da.
- Zerbitzuaren ukapenaren edo 800xA Sistemaren nodoen manipulazioaren arriskua dago. Hori baliatuz erasotzaile batek sistemaren nodoa irisgarri utz lezake, edo sistemaren exekuzio denboran datuak manipulatu. Larritasun ertain eta altuko ahultasun hauetarako CVE-2020-8478, CVE-2020-8484, CVE-2020-8485, CVE-2020-8486, CVE-2020-8487, CVE-2020-8488 eta CVE-2020-8489 identifikatzaileak erabili dira.

Etiketak: Ahultasuna

Bideetara kontrolatu gabeko sarbidea ABBren UPS Adapter CS141-en

Argitalpen data: 2020/04/24

Garrantzia: Ertaina

Kaltetutako baliabideak:

- UPS Adapter CS141en ondoko gailuak, firmware-aren bertsioa 1.66tik 1.88ra bitartekoa dutenak:
  - CS141 Advanced - Box;
  - CS141 Advanced - Slot;
  - CS141 ModBus - Box;
  - CS141 ModBus - Slot;
  - CS141 Basic - Box;
  - CS141 Basic - Slot.

Azalpena:

Eduardo Cataño Conde zibersegurtasun ikertzaileak ABBri kritikotasun ertaineko ahultasun baten berri eman dio. Hori baliatuz urruneko erasotzaile batek bideetara sarbide ez kontrolatua lor lezake eta kaltetutako gailuaren informazioa eskuratu.

Konponbidea:

Kaltetutako produktuak firmware-aren 1.90 bertsiora eguneratzea.

Xehetasuna:

Administratzaile edo ingeniari kredentzialak lituzkeen erasotzaile batek fitxategietara erreferentzia egiten duten aldaerak manipula litzake, "web" direktoriotik kanpoko direktorio eta fitxategietara sarbidea lortzeko. Ahultasun horretarako CVE-2020-11420 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Informazioaren hedapena Moxa-ren NPort 5100A Series-en

Argitalpen data: 2020/04/29

Garrantzia: Ertaina

Kaltetutako baliabideak:

NPort 5100A Series, *firmware*-aren 1.5 bertsioa edo lehenagokoa.

Azalpena:

Moxaren NPort 5100A Series produktuek duten ahultasun bat argitaratu da. Hori baliatuz autentifikatu gabeko erasotzaile batek informazioa zabal lezake.

Konponbidea:

- *Firmware*-aren 1.51 edo geroagoko bertsioetara eguneratzea.
- Ezarpenen kontsolatik "Moxa Service" aukera desgaitzea. Aukera hori behar izanez gero, sarbidea behar duten gailuak zerrenda zuri batera gehitzea, eta "Accessible IP List"-eko zerrenden konfigurazioan 'Apply additional restrictions' aukera aktibatzea.

Xehetasuna:

Ahultasuna baliatuz autentifikatu gabeko erasotzaile batek gailuaren serie atakaren konfigurazioak eskura litzake. Ahultasun horretarako CVE-2020-12117 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna