2020ko otsailaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Ondo babestu gabeko kredentzialak AutomationDirect-en C-more Touch Panels-en

Argitalpen data: 2020/02/05

Garrantzia: Kritikoa

Kaltetutako baliabideak:

C-More Touch Panels EA9 series, *firmware*-aren 6.53 eta lehenagoko bertsioak.

Azalpena:

Amentum Mission Engineering & Resilience-ko Joel Langill ikertzaileak ondo babestu gabeko kredentzial erako ahultasun baten berri eman du. Hori baliatuz erasotzaile batek kontuaren informazioa eskura lezake, esate baterako erabiltzaile izenak eta pasahitzak, prozesuaren datuak ezkutatu edo manipulatu litzake eta gailurako sarbidea blokeatu.

Konponbidea:

Fabrikatzaileak gomendatzen du 6.53 bertsiora eguneratzea.

Xehetasuna:

Identifikatutako ahultasuna baliatuz urruneko erasotzaile batek babestu gabeko proiektuetan kredentzialak eskura litzake, bai eta beste informazio sentikor bat ere. Horrela sistemara sarbidea lortuko luke, eta bere konfigurazioa manipula lezake. Ahultasun horretarako CVE-2020-6969 kodea erreserbatu da.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Ahultasuna

Bufferraren gainezkatzea Philips-en bonbilla inteligenteetan

Argitalpen data: 2020/02/05

Garrantzia: Altua

Kaltetutako baliabideak:

Philips HUE bonbilla inteligenteak.

Azalpena:

Check Point-eko ikertzaileek ahultasun baten berri eman dute, memoria dinamikoan (Heap) oinarritutako bufferraren gainezkatze erakoa.

Konponbidea:

Kaltetutako produktuen firmwarearen 1935144040 bertsioa argitaratu da, ahultasun hori konpontzen duena. Eguneraketaren instalazioa automatikoa da. Nolanahi ere, gailua eguneratu egin dela egiaztatzea aholkatzen da. Bestela eskuz egin beharra dago.

Xehetasuna:

Identifikatutako ahultasuna baliatuz, erasotzaile batek bonbillen IoT sarearen kontrola har lezake, kontrol zubira datu kopuru handiak bidaliz. Horrela malware erasoak egin litzake enpresen sare informatikoen aurka, eta baita hiri inteligenteen aurka ere. Ahultasun horretarako CVE-2020-6007 kodea erreserbatu da.

Etiketak: IoT, Ahultasuna

Hainbat ahultasun Meinberg-en LANTIME-n

Argitalpen data: 2020/02/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- LANTIMEren V6.24.024 (V7.00.002 hurrenez hurren) baino lehenagoko firmware-aren bertsio guztiak, salbu eta CVE-2019-1551 eta NO-CVE13, horiek V7.00.006 baino lehenagoko bertsio guztiei ere eragiten baitiete;
- LANTIMEren M serieko gailu guztiak (M100, M200, M300, M400, M600, M900);
- LANTIMEren IMS serieko gailu guztiak (M500, M1000, M1000S, M3000, M3000S, M4000);
- SyncFire produktuen familia (SF1000 / SF1100).

Azalpena:

Checkpoint-eko Michal Bazyli eta Jakub Palaczynski ikertzaileek hainbat eratako ahultasunen berri eman dute: fitxategi arbitrarioen irakurketa/idazketa, pribilegioen eskalatzea, informazioaren hedapena, kodearen urruneko exekuzioa, nabigatzailearen cachearen ahultasuna, komandoen online injekzioa, bufferraren gainezkatzea, informazio sentikorraren zifratze falta eta lehenetsitako SSH pasahitza.

Konponbidea:

Firmware-a V7.00.006 eta V6.24.024 bertsioetara eguneratzea deskargen zentrotik aipatutako ahultasunak konpontzeko, salbu eta CVE-2020-7240 identifikatzailea duen ahultasuna.

Xehetasuna:

Ondoren zehazten dira larritasun kritikoko ahultasunak:

- Autentifikatu gabeko erabiltzaileek Java Script kodea alda dezakete saio hasierako elkarrizketa koadrotik, web zerbitzariak emandako System → System Information → Show System Messages funtzioaren bidez, gordetako eta autentifikatu gabeko XSS eraso bat eginez.
- TSUko txarteletarako root sarbidea sarearen bidez egitea posible zen SSHren lehenetsitako gako bat mantentzen zelako.

Gainerako ahultasunetarako honako identifikatzaileak erreserbatu dira: CVE-2018-10834, CVE-2018-10835 eta CVE-2018-10836.Esleitutako identifikatzaileak honakoak dira: CVE-2020-7240, CVE-2011-2900, CVE-2019-1563, CVE-2019-1547, CVE-2019-1552 eta CVE-2019-1551.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Komunikazioak, Ahultasuna

XSS erako ahultasuna eWON-en hainbat produktutan

Argitalpen data: 2020/02/11

Garrantzia: Altua

Kaltetutako baliabideak:

- Flexy, 14.1s0 baino lehenagoko bertsioak;
- Cosy, 14.1s0 baino lehenagoko bertsioak.

Azalpena:

Titanium Industrial Security-ko Ander Martinezek eWon gailuek duten ahultasun baten berri eman du. Hori baliatuz, urruneko erasotzaile batek CSRF eraso bat egin lezake, administratzailearen makina arriskuan jarriz.

Konponbidea:

14.1s0 bertsiora eguneratzea.

Xehetasuna:

Erasotzaile batek pasahitza alda lezake CSRF erako eraso bat eginez, edo administratzailearen makina arriskuan jar lezake nabigatzailearen ahultasunen bat erabiliz. XSSren biktimak kredentzialak sartu behar ditu kodea exekutatu baino lehen.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Siemens gailuetan

Argitalpen data: 2020/02/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- OpenPCS 7, SIMATIC BATCH, SIMATIC PCS 7 eta SIMATIC Route Control:
  - V8.1, bertsio guztiak;
  - V8.2, bertsio guztiak;
  - V9.0, bertsio guztiak.
- SIMATIC NET PC Software;

- SIMATIC WinCC (TIA Portal):
  - V13, V13 SP2 bertsioak baino lehenagokoak;
  - V14.0.1, bertsio guztiak;
  - V15.1, bertsio guztiak;
  - V16, bertsio guztiak.
- SIMATIC WinCC:
  - V7.3, bertsio guztiak;
  - V7.4, bertsio guztiak;
  - V7.5, V7.5.1 Udp1 baino lehenagoko bertsioak.
- SIMATIC S7-1200 vamilia, SIPLUS aldaera barne, V4.1 bertsioa baino lehenagokoak;
- SIMATIC S7-300 PN/DP CPU familia, SIPLUS aldaera barne, eta ET200 CPUekin erlazionatutakoak, bertsio guztiak;
- SIMATIC S7-400 PN/DP V6 familia, SIPLUS aldaera barne, bertsio guztiak;
- SIMATIC S7-400 PN/DP V7 CPU familia eta lehenagokoak, SIPLUS aldaera barne, bertsio guztiak;
- SCALANCE:
  - S602, bertsio guztiak;
  - S612, bertsio guztiak;
  - S623, bertsio guztiak;
  - S627-2M, bertsio guztiak.
- SIMATIC ET 200SP Open Controller CPU 1515SP PC2, SIPLUS aldaera barne, bertsio guztiak;
- SIMATIC S7-1500 CPU familia, SIPLUS aldaera barne, eta ET200 CPUekin erlazionatutakoak, V2.5 baino lehenagoko bertsio guztiak, hori barne, eta V2.5 eta V2.8 bitarteko bertsioak;
- SIMATIC S7-1500 Software Controller. V2.5 baino lehenagoko bertsio guztiak, bera barne, eta V2.5 eta V20.8 bitarteko bertsioak;
- SIMATIC CP-1623, V14.00.15.00_51.25.00.01 bertsioa baino lehenagoko guztiak;
- SIMATIC CP 1626, bertsio guztiak;
- SIMATIC CP 1628, bertsio guztiak;
- TIM 1531 IRC (SIPLUS NET aldaera guztiak barne), V2.0 baino lehenagoko bertsio guztiak;
- PROFINET IOrako garapen/ebaluazio kit-ak:
  - DK Standard Ethernet Controller, bertsio guztiak;
  - EK-ERTEC 200, V4.5 baino lehenagoko bertsioak;
  - EK-ERTEC 200P, V4.6 baino lehenagoko bertsioak.
- PROFINET Driver for Controller, V2.1 bertsioa baino lehenagokoak;
- IE/PB LINK PN IO (SIPLUS NET aldaera guztiak barne);
- RUGGEDCOM RM1224, V4.3 bertsioa baino lehenagokoak;
- SIPORT MP, 3.1.4 baino lehenagoko bertsio guztiak;
- OZW672, v10.00 bertsioaren aurreko guztiak;
- OZW772, v10.00 bertsioaren aurreko guztiak;
- SCALANCE:
  - M-800 / S615, V4.3 baino lehenagoko bertsioak;
  - W700 IEEE 802.11n, V6.0.1 baino lehenagoko bertsioak, bera barne;
  - X-200 switchen familia, SIPLUS NETen aldaera barne, bertsio guztiak;
  - X-200IRT switchen familia, SIPLUS NETen aldaera barne, bertsio guztiak;
  - X-300 switchen familia, SIPLUS NETen aldaera eta X408 barne, bertsio guztiak;
  - XB-200, XC-200, XP-200, XF-200BA eta XR-300WG, V3.0 baino lehenagoko bertsioak;
  - XM-400 switchen familia, V6.0 baino lehenagoko bertsioak;
  - XR-500 switchen familia, V6.0 baino lehenagoko bertsioak.
- SIMATIC:
  - CP 1616 eta CP 1604, V2.8 baino lehenagoko bertsioak;
  - CP 343-1, SIPLUS NETen aldaera barne, bertsio guztiak;
  - CP 343-1 Advanced, SIPLUS NETen aldaera barne, bertsio guztiak;
  - CP 343-1ERPC, bertsio guztiak;
  - CP 343-1LEAN, bertsio guztiak;
  - CP 443-1, SIPLUS NETen aldaera barne, bertsio guztiak;
  - CP 443-1 Advanced, SIPLUS NETen aldaera barne, bertsio guztiak;
  - CP 443-1 OPC UA, bertsio guztiak;
  - ET200AL;
  - ET200ecoPN (salbu eta 6ES7148-6JD00- 0AB0 eta 6ES7146-6FF00-0AB0), bertsio guztiak;
  - ET200S, SIPLUS aldaera barne, bertsio guztiak;
  - ET200S, SIPLUS aldaera barne, bertsio guztiak;
  - ET200M, SIPLUS aldaera barne, bertsio guztiak;
  - SIMATIC CP 1543-1, V2.0 baino lehenagoko bertsioak eta V2.0 eta V2.2 bitartekoak;
  - IPC Support, VxWork-erako paketea, bertsio guztiak;
  - MV400 familia, bertsio guztiak;
  - RF182C, bertsio guztiak;
  - RF600 familia, V3 baino lehenagoko bertsioak.
- SINAMICS DCP, V1.3 baino lehenagoko bertsioak;
- SIPROTEC 4 eta SIPROTEC Compact erreleak, bertsio guztiak.

Azalpena:

Ohartarazpen honek Siemensen hainbat produkturi eragiten dieten 15 ahultasun jasotzen ditu, horietatik 1 larritasun kritikokoa da, 8 larritasun altukoak eta 6 larritasun ertainekoak.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak Siemens-en deskarga panelean eskura daitezke.

Eguneraketarik eskuragarri ez daukaten produktuen kasuan erreferentzien atalean azaltzen diren arintze neurriak ezarri behar dira.

Xehetasuna:

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

- Zerbitzuaren ukapena,
- Kodearen urruneko exekuzioa,
- Informazioa zabaltzea.

Ahultasun horietarako honako identifikatzaileak erabili dira: CVE-2019-19282, CVE-2019-13925, CVE-2019-3926, CVE-2019-19281, CVE-2019-13946, CVE-2019-12815, CVE-2019-18217, CVE-2019-19279, CVE-2015-5621, CVE-2019-13940, CVE-2019-6585, CVE-2019-13924, CVE-2018-18065, CVE-2019-19277 eta CVE-2019-13941.

Etiketak: Eguneraketa, Siemens, Ahultasuna

Hainbat ahultasun Digi International-en ConnectPort LTS 32 MEI-n

Argitalpen data: 2020/02/12

Garrantzia: Txikia

Kaltetutako baliabideak:

ConnectPort LTS 32 MEI, firmwarearen 1.4.3 bertsioa (82002228_K 08/09/2018) eta bios-aren 1.2 bertsioa.

Azalpena:

Murat Aydemir eta Fatih Kayran ikertzaileek Digi International-en ConnectPort LTS 32 MEI produktuak dituen hainbat ahultasunen berri eman dute. Horiek baliatuz, erasotzaile batek sistemaren eskuragarritasuna muga lezake.

Konponbidea:

1.4.5 bertsiora eguneratzea.

Xehetasuna:

- Fitxategiak murrizpenik gabe igo ahal izatea baliatuz, erasotzaile batek asmo gaiztoko kodea sar lezake aplikazioan. Ahultasun horretarako CVE-2020-6975 identifikatzailea erabili da.
- Web orria sortzen denean sarreraren neutralizazio okerra baliatuz, erasotzaile batek zerbitzuaren ukapen egoera eragin lezake cross-site scripting erako erasoen bidez. Ahultasun horretarako CVE-2020-6973 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Bilaketa bide ez-kontrolatua Schneider Electric-en ProSoft Configurator-en

Argitalpen data: 2020/02/12

Garrantzia: Altua

Kaltetutako baliabideak:

ProSoft Configurator v1.002 eta lehenagokoak, PMEPXM0100 (H) modulurako.

Azalpena:

Yongjun Liu (nsfocus) ikertzaileak kontrolatu gabeko bilaketa bide erako ahultasun bat aurkitu du, ProSoft Configurator-i eragiten diona. Hori baliatuz erasotzaile lokal batek kode arbitrarioa exekuta lezake.

Konponbidea:

ProSoft Configurator v1.003 bertsiora edo berriago batera eguneratzea.

Xehetasuna:

Kontrolatu gabeko bilaketa bidearen (path) elementuko ahultasun bat baliatuz, erasotzaile lokal batek kode arbitrarioa exekuta lezake proiektu bat irekitzean, asmo gaiztoko DLL bat exekuta lezakeena. Ahultasun horretarako CVE-2020-7474 identifikatzailea erreserbatu da.

Etiektak: Eguneraketa, Ahultasuna

Hainbat ahultasun ABBren produktuetan

Argitalpen data: 2020/02/13

Garrantzia: Altua

Kaltetutako baliabideak:

- Asset Suite, 9.6 eta lehenagoko bertsioak.
- eSOMS, 6.02 eta lehenagoko bertsioak.

Azalpena:

ABBk era hauetako hainbat ahultasunen berri eman du: objektura erreferentzia zuzena, zuzen aktibatu gabeko HTTP goiburuak, aktibatu gabeko flag ez-seguruak, informazioaren filtrazioa, pasahitzaren konplexutasunaren kontrol falta, software ahularen erabilpena, SQL injekzioa, sarreren eta irteeren baliozkotze falta, pasahitzak lauan gordetzea eta enkriptatze ahuleko algoritmoen erabilpena. Ahultasun hauek baliatuz erasotzaile batek informazio sentikorrera sarbidea lor lezake.

Konponbidea:

Honako bertsio hauetara eguneratzea:

- eSOMS: 6.0.3 eta 6.1,
- Asset Suite: 9.4.2.6, 9.5.3.2 eta 9.6.1.

Xehetasuna:

Larritasun altuko ahultasunak honakoak dira:

- Baliabideetarako sarbidea mugatzeko erabiltzen diren kontroletako ahultasun bat baliatuz, erasotzaile batek erabiltzeko baimenik ez duen baliabide baten URLa ezagutzen edo aurkitzen badu, baliabide horretara sarbidea lor lezake URLaren bitartez hura zuzenean bilatuz. Ahultasun horretarako CVE-2019-18998 identifikatzailea erabili da.
- eSOMS-en Redis-en bertsio ahul bat instalatuta dago.
- eSOMS-en SQL query-etarako sarreraren baliozkotze falta baliatuz, erasotzaile batek SQL injekzio erako erasoak egin litzake barneko datu basearen aurka. Ahultasun horretarako CVE-2019-19094 identifikatzailea erabili da.

Gainerako ahultasunetarako identifikatzaile hauek esleitu dira: CVE-2019-19000, CVE-2019-19001, CVE-2019-19002, CVE-2019-19003, CVE-2019-19089, CVE-2019-19090, CVE-2019-19091, CVE-2019-19092, CVE-2019-19093, CVE-2019-19095, CVE-2019-19096 eta CVE-2019-19097.

Etiketak: Ahultasuna

Hainbat ahultasun Moxa-ren OnCell ekipoetan

Argitalpen data: 2020/02/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Moxa OnCell G3470A-LTE Series, firmware-aren 1.6 edo lehenagoko bertsioak.
- Moxa OnCell G3100-HSPA Series, firmware-aren bertsio hauek:
  - 1.4 edo lehenagokoak, CVE-2018-11420, CVE-2018-11423 eta CVE-2018-11424 identifikatzaileak dituzten ahultasunetarako;
  - 1.7 edo lehenagokoak, CVE-2018-11426, CVE-2018-11427, CVE-2018-11421 eta CVE-2018-11422 identifikatzaileak dituzten ahultasunetarako.

Azalpena:

Kaspersky Lab-eko Alexander Zaytsev-ek Moxa-ren OnCell G3470A-LTE Series eta OnCell G3100-HSPA produktuei eragiten dieten era hauetako hainbat ahultasunen berri eman dute: eragiketen murrizpen desegokia, baliabideen kontrolik gabeko kontsumoa, NULL erakuslearen deserreferentzia, autentifikazio desegokia, CSRF, informazioaren hedapena eta sarbidearen kontrol desegokia.

Konponbidea:

- OnCell G3470A-LTE Series-en kasuan, produktuaren firmware-aren azken bertsioa deskargatzea.
- OnCell G3100-HSPA Series-en kasuan
  - produktuaren firmware-aren azken bertsioa deskargatzea, CVE-2018-11420, CVE-2018-11423, CVE-2018-11424, CVE-2018-11426 eta CVE-2018-11427 identifikatzaileak dituzten ahultasunak konpontzeko;
  - puntutik punturako VPN soluzioak bezalako segurtasun neurriak gehitzea, soilik kaltetutako produktuan OnCell Search Utility eta OnCell Central Manager funtzionaltasunak aktibatuta daudenean, CVE-2018-11421 eta CVE-2018-11422 identifikatzaileak dituzten ahultasunak konpontzeko.

Xehetasuna:

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

- zerbitzuaren ukapena,
- kodearen urruneko exekuzioa,
- autentifikazio parametroen aurkako indar hutseko erasoak,
- web interfazearen bidez ekintza administratiboak ordeztea,
- informazio sentikorra eskuratzea,
- konfigurazioak aldatzea eta firmware-a igotzea.

Honako identifikatzaile hauek esleitu dira: CVE-2018-11420, CVE-2018-11421, CVE-2018-11422, CVE-2018-11423, CVE-2018-11424, CVE-2018-11425, CVE-2018-11426 eta CVE-2018-11427.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Web zerbitzarira autentifikatu gabeko sarbidea Phoenix Contact-en produktuetan

Argitalpen data: 2020/02/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Phoenix Contact Emalytics Controllers ILC 2050 BI, firmware-aren 1.21 bertsiora artekoak;
- Phoenix Contact Emalytics Controllers ILC 2050 BI-L, firmware-aren 1.21 bertsiora artekoak.

Azalpena:

Anil Parmar-ek ahultasun kritiko bat aurkitu du, urruneko konfigurazio erakoa web zerbitzari batera autentifikatu gabeko sarbide bat erabiltzen denean, Phoenix Contact-en hainbat produkturi eragiten diena.

Konponbidea:

Kaltetutako produktuak firmware-aren 1.2.3 bertsiora edo goragoko batera eguneratzea.

Xehetasuna:

Kaltetutako gailuek webera duten esteka batek baimendu gabeko sarbidea ematen du gailu horien konfiguraziora, irakurketa eta idazketa baimenekin. Hori baliatuz erasotzaile batek gailuen konfigurazioa alda lezake eta zerbitzuak abiarazi eta gelditu. Ahultasun horretarako CVE-2020-8768 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Azpiegitura kritikoak, Ahultasuna

---

Pribilegioen kudeaketa okerra Honeywell-en INNCOM INNControl 3-n

Argitalpen data: 2020/02/19

Garrantzia: Ertaina

Kaltetutako baliabideak:

INNControl 3, 3.21 eta lehenagoko bertsioak

Azalpena:

Honeywell-eko ekipoak ahultasun baten berri eman du, pribilegioen kudeaketa oker erakoa, bere INNCOM INNControl 3 produktuari eragiten diona.

Konponbidea:

Erabiltzaileak harremanetan jarri behar dira INNCOM-eko salmenta ordezkari batekin edo baimendutako sistema integratzaile batekin, beren sistema azken bertsiora eguneratzeko informazioa eskuratzearren. Honeywell-ek INNCOMen online zerbitzua ere eskaintzen du.

Xehetasuna:

Aurkitutako ahultasuna, pribilegioen kudeaketa oker erakoa, baliatuz gero, erasotzaile batek erabiltzaile pribilegioak igo litzake INNControl aplikazioaren barnean, konfigurazio lokaleko fitxategiak aldatuz. Ahultasun horretarako CVE-2020-6968 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Azpiegitura Kritikoak, Osasuna, Ahultasuna

---

Babes mekanismoaren akatsa GEren hainbat produktutan

Argitalpen data: 2020/02/19

Garrantzia: Ertaina

Kaltetutako baliabideak:

- Vivid, bertsio guztiak;
- LOGIQ, bertsio guztiak salbu eta LOGIQ 100 Pro;
- Voluson, bertsio guztiak;
- Versana Essential, bertsio guztiak;
- Invenia ABUS Scan station, bertsio guztiak;
- Venue, bertsio guztiak, ez ordea Venue 40 R1-3 eta Venue 50 R4-5.

Azalpena:

Marc Ruef eta Rocco Gagliardi ikertzaileek babes mekanismoaren akats erako ahultasun baten berri eman dute. Hori baliatuz erasotzaile batek kaltetutako gailuaren sistema eragilera sarbidea eskura lezake.

Konponbidea:

GE Healthcare-k erakundeei gomendatzen die baimenik gabeko pertsonei gailuetarako sarbide fisikoa murriztea, eta posible bada, GUI-an pasahitz bidez gailuaren blokeoa aktibatzea.

Xehetasuna:

Kiosk moduaren funtzionaltasunak duen mahaigaineko ingurune murriztutik ihes erako ahultasun bat baliatuz, erasotzaile batek ingurune murriztutik ihes egin lezake eta azpiko sistema eragilera sarbidea lortu, bereziki diseinatutako sarreren bidez. CVE-2020-6977 identifikatzailea esleitu zaio.

Etiketak: Ahultasuna

Memoria dinamikoan oinarritutako bufferraren gainezkatzea Emerson-en OpenEnterprise-n

Argitalpen data: 2020/02/19

Garrantzia: Altua

Kaltetutako baliabideak:

- OpenEnterprise Server 2.83 kaltetua dago Modbus edo ROC Interfaces protokoloak instalatuak izan badira eta erabiltzen ari

badira;
- OpenEnterprise, 3.1etik 3.3.3ra bitarteko bertsio guztiak.

Azalpena:

Kaspersky ICS CERT-eko Roman Lozko-k memoria dinamikoan (heap) oinarritutako bufferraren gainezkatze erako ahultasun baten berri eman du, Emerson-en OpenEnterprise produktuari eragiten diona.

Konponbidea:

OpenEnterprise 3.3 SP4 (3.3.4) bertsiora eguneratzea, Emerson-en zerbitzu webean eskuragarri.

Xehetasuna:

Bereziki diseinatutako *script* bat balia daiteke kodea exekutatzeko OpenEnterprise-ren zerbitzarian, eta horrela memoria dinamikoan (heap) oinarritutako bufferraren gainezkatzea eragingo litzateke. Ahultasun horretarako CVE-2020-6970 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Azpiegutra Kritikoak, Ahultasuna

Baimentze desegokia B&R Industrial Automation GmbH-ren hainbat produktutan

Argitalpen data: 2020/02/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Automation Studio, honako bertsioak:
  - 2.7;
  - 3.0.71;
  - 3.0.80;
  - 3.0.81;
  - 3.0.90;
  - 4.6.4tik 4.0.x-era bitartekoak;
  - 4.7.2.
- Automation Runtime, honako bertsioak:
  - 2.96;
  - 3.00;
  - 3.01;
  - 3.06;
  - 3.07;
  - 3.08 bertsiotik 3.10 bertsiora bitartekoak;
  - 4.00 bertsiotik 4.03 bertsiora bitartekoak;
  - 4.04 bertsiotik 4.03 bertsiora bitartekoak;
  - 4.04 bertsiotik 4.63 bertsiora bitartekoak;
  - 4.72 eta goragokoak.

Azalpena:

Claroty-ko Yehuda Anikster eta Amir Preminger-ek larritasun kritikoko ahultasun baten berri eman dute, baimentze desegoki erakoa, B&R Industrial Automation GmbH-en hainbat produkturi eragiten diena.

Konponbidea:

B&R-k jakinarazi du produktuaren arrazoi teknikoengatik ez dutela onartzen SNMP kredentzialen aldaketa. Ahultasun honen arriskua murrizteko, Automation Studio-ren ondoko bertsioek lehenetsitako SNMP zerbitzua desgaitzen dute sortu berri diren AS proiektuetan:

- AS 4.6.5 (aurreikusitako argitalpen data: 2020/03/27) eta goragokoak;
- AS 4.7.3 (aurreikusitako argitalpen data: 2020/04/10) eta goragokoak;
- AS 4.8.2 (aurreikusitako argitalpen data: 2020/06/11) eta goragokoak.

Xehetasuna:

Kaltetutako produktuak ahulak dira SNMP zerbitzuak duen ahultasun baten aurrean. Hori baliatuz autentifikatu gabeko urruneko erasotzaile batek kaltetutako gailuen konfigurazioa alda lezake. Ahultasun horretarako CVE-2019-19108 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Azpiegitura Kritikoak, Ahultasuna

Hainbat ahultasun Honeywell-en Notifier Web Server-en (NWS-3)

Argitalpen data: 2020/02/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Honeywell Notifier Web Server (NWS-3), 3.50 eta lehenagoko bertsioak.

Azalpena:

Gjoko Krstikj-ek larritasun kritikoko bi ahultasunen berri eman du, bat sareko trafikoa atzeman eta errepikatzeagatik autentifikazio falta erakoa, eta bestea bideetarako kontrolik gabeko sarbide erakoa.

Konponbidea:

Kaltetutako produktua firmware-aren 4.51 bertsiora eguneratzea.

Xehetasuna:

- Honeywell Fire Web Server-eko autentifikazioa saihestu egin daiteke sareko trafikoa atzeman eta errepikatzeko eraso batengatik web nabigatzaile batetik. Ahultasun horretarako CVE-2020-6972 identifikatzailea erreserbatu da.
- Kaltetutako produktua ahula da bideetara kontrolatu gabeko sarbide erako eraso baten aurrean. Hori baliatuz erasotzaile batek direktorio murriztuetarako sarbidea saihets lezake. Ahultasun horretarako CVE-2020-6974 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Ahultasuna Rockwell Automation-en FactoryTalk Diagnostics-en

Argitalpen data: 2020/02/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- FactoryTalk Diagnostics, bertsio guztiak.

Azalpena:

Fidagarriak ez diren datuen deserializazio erako ahultasun baten berri eman da. Hori baliatuz erasotzaile batek kode arbitrarioa exekuta lezake SYSTEM pribilegioekin.

Konponbidea:

Rockwell Automation eguneraketa bat prestatzen ari da. Ordura arte ondokoa gomendatzen da:

- Remote Deshabilitar zerbitzua erabiltzen ez bada desgaitzea;
- Zerbitzua erabiltzen ari bada, firewall bat erabiltzea kaltetutako ataka desgaitzeko.

Xehetasuna:

Factory Talk Diagnostics-ek Remoting endpoint .NET agerian uzten du, RNADiagnosticsSrv.exe-ren bidez TCP/8082-n, eta horrek fidagarriak ez diren datuak modu ez-seguruan deserializa ditzake. CVE-2020-6967 identifikatzailea esleitu zaio.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Moxa-ren AWK-3131A Series-en

Argitalpen data: 2020/02/24

Garrantzia: Altua

Kaltetutako baliabideak:

AWK-3131A Series, firmware-aren 1.13 eta lehenagoko bertsioak.

Azalpena:

Moxaren produktuetan hainbat eratako ahultasunak aurkitu dira: sarbide kontrol desegokia, barneratutako pasahitzen erabilpena, sistema eragilearen komandoetan erabilitako elementu berezien neutralizazio desegokia, bufferra kopiatzea sarrera tamainaren egiaztapenik gabe, mugez kanpoko irakurketa, pilan (stack) oinarritutako bufferraren gainezkatzea eta autentifikazioa saihestea kanal edo bide alternatiboaren bidez.

Konponbidea:

Moxaren zerbitzu teknikoarekin harremanetan jartzea eguneraketa eskuratzeko.

Xehetasuna:

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

- Komandoan bidaltzea. Ahultasun horietarako CVE-2019-5136 eta CVE-2019-5162 identifikatzaileak erreserbatu dira.
- Atzemandako trafikoa deszifratzea. Ahultasun horretarako CVE-2019-5137 identifikatzailea erreserbatu da.
- Komandoen injekzioa gailuaren kontrola eskuratzeko. Ahultasun horietarako CVE-2019-5138, CVE-2019-5140, CVE-2019-5141 eta CVE-2019-5142 identifikatzaileak erreserbatu dira.
- Pasahitz barneratuen erabilpena. Ahultasun horretarako CVE-2019-5139 identifikatzailea erreserbatu da.
- Kodearen urruneko exekuzioa. Ahultasun horietarako CVE-2019-5143 eta CVE-2019-5153 identifikatzaileak erreserbatu dira.
- Zerbitzuaren ukapena. Ahultasun horretarako CVE-2019-5148 identifikatzailea erreserbatu da.
- Autentifikazioari ihes egitea. Ahultasun horretarako CVE-2019-5165 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Honeywell WIN-PAK-en produktuetan

Argitalpen data: 2020/02/26

Garrantzia: Altua

Kaltetutako baliabideak:

WIN-PAK,4.7.2 bertsioa eta lehenagokoak.

Azalpena

3 ahultasun aurkitu dira, 2 larritasun altukoak eta bat ertainekoa, era ezberdinekoak: CSRF, script-en sintaxietarako HTTP goiburuen neutralizazio desegokia eta liburutegi zaharkituen erabilpena.

Konponbidea:

WIN-PAK 4.7.2 B1072.3.4 bertsiora eguneratzea eta ondoren partxea ezartzea.

Xehetasuna:

- Kaltetutako produktua ahula da CSRFren (Cross-Site Request Forgery) aurrean eta hori baliatuz urruneko erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2020-7005 identifikatzailea erreserbatu da.
- HTTP goiburuen neutralizazio oker erako ahultasun bat aurkitu da. Hori baliatuz kodearen urruneko exekuzioa egin liteke. Ahultasun horretarako CVE-2020-6982 identifikatzailea erreserbatu da.
- Kaltetutako produktua ahula da zaharkitutako jQuery liburutegiak erabiltzen direlako. Ahultasun horretarako CVE-2020-6978 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Azpiegitura Kritikoak, Ahultasuna

Hainbat ahultasun Moxa-ren produktuetan

Argitalpen data: 2020/02/26

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Protokoloen pasarela hauek:
  - 4.0. bertsioko firmwarea edo lehenagokoa duten MB3170 serieak;
  - 4.0. bertsioko firmwarea edo lehenagokoa duten MB3270 serieak;
  - 2.0. bertsioko firmwarea edo lehenagokoa duten MB3180 serieak;
  - 3.0. bertsioko firmwarea edo lehenagokoa duten MB3280 serieak;
  - 3.0. bertsioko firmwarea edo lehenagokoa duten MB3480 serieak;
  - 2.2. bertsioko firmwarea edo lehenagokoa duten MB3660 serieak.
- 3.0. bertsioko firmwarea edo lehenagokoa duten ioLogik 2500 serieak;
- IOxpress konfigurazio zerbitzua, 2.3.0 edo lehenagoko bertsioa;
- Ethernet switch hauek:
-
  - 4.0. bertsioko firmwarea edo lehenagokoa duten PT-7528 serieak;
  - 3.9. bertsioko firmwarea edo lehenagokoa duten PT-7828 serieak;
  - 5.2. bertsioko firmwarea edo lehenagokoa duten DS-G516E serieak;
  - 5.2. bertsioko firmwarea edo lehenagokoa duten EDS-510E serieak.

Azalpena:

Hainbat ikertzailek Moxa-ri hogeita bost ahultasunen berri eman diote, bat larritasun baxukoa, sei ertainekoak, zortzi altukoak eta hamar larritasun kritikokoak. Urruneko erasotzaile batek kode arbitrarioa exekuta lezake, sarbide murrizpenak saihestu eta konfigurazioak aldatu. Horrela konfidentzialtasunari, integritateari eta eskuragarritasunari eragingo litzaieke.

Konponbidea:

- EDS-G516E serieen kasuan, eskuragarri dagoen azken bertsiora eguneratzea gomendatzen da.
- MOXAk firmware bertsio berri bat garatu du honako modeloentzat: MB3170, MB3270, MB3180, MB3280, MB3480 eta MB3660.Eskuratzeko, zuzenean harremanetan jarri beharra dago fabrikatzailearekin eguneratu ahal izateko.
- Gainerako gailuen kasuan kontsultatu Moxa-ren zerbitzu teknikoa.

Xehetasuna:

- Erasotzaile batek kode arbitrarioa exekuta lezake, gailua zerbitzuz kanpo utziz. Ahultasun horietarako CVE-2020-7007, CVE-2020-6989 eta CVE-2019-9099 identifikatzaileak erreserbatu dira.
- Kaltetutako produktuek barneratutako gako kriptografikoak erabiltzen dituzte, eta horrek informazio konfidentziala ezagutzera ematea ahalbidetu lezake. Ahultasun horietarako CVE-2020-6979 eta CVE-2020-6983 identifikatzaileak erreserbatu dira.
- Erasotzaile batek sistemarako sarbidea lor lezake baimen egokirik gabe. Ahultasun horietarako CVE-2020-6981 eta CVE-2020-6985 identifikatzaileak erreserbatu dira.
- Erasotzaile batek sistemara sarbidea lor lezake indar gordina erabiliz. Ahultasun horietarako CVE-2020-6991, CVE-2020-6995 eta CVE-2019-9096 identifikatzaileak erreserbatu dira..

Gainerako ahultasunetarako honako identifikatzaileak esleitu dira: CVE-2020-7001, CVE-2020-6989, CVE-2020-6997, CVE-2020-6987, CVE-2020-6993, CVE-2019-18238, CVE-2020-7003, CVE-2019-18242, CVE-2019-9098, CVE-2019-9102, CVE-2019-9095, CVE-2019-9103, CVE-2019-9101, CVE-2019-9104 eta CVE-2019-9097.

Etiketak: Eguneraketa, Ahultasuna

Bufferraren gainezkatzea Advantech-en WebAcces/SCADAn

Argitalpen data: 2020/02/27

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Advantech WebAccess/SCADA, 8.4.3 bertsioa.

Azalpena:

Bufferraren gainezkatze erako larritasun kritikoko ahultasun bat aurkitu da, Advantech-en WebAccess/SCADA softwareari eragiten diona. Ahultasun hori arrakastaz baliatuz gero, urruneko erasotzaile batek kode arbitrarioa exekuta lezake.

Konponbidea:

Advantech-ek softwarearen 9.0 bertsioa argitaratu du, ahultasun hori konpontzen duena.

Xehetasuna:

BwPAlarm.dll liburutegian ez da egiten erabiltzailearen datuen baliozkotze zuzen bat IOCTL 70022 RPC erako mezuak prozesatzen direnean. Hori baliatuz urruneko erasotzaile batek pilaren bufferraren tamaina kontrola lezake, baita bertan kopiatutako datuak ere.

Etiketak: Eguneraketa, SCADA, Ahultasuna