2020ko Maiatzaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Hainbat ahultasun SAE IT-systems-en FW-50 RTU-n

Argitalpen data: 2020/05/06

Garrantzia: Kritikoa

Kaltetutako baliabideak:

W-50 RTU, 5 Series, CPU-5B, Hardware Revision: 2, CPLD Revision: 6.

Azalpena:

FW-50 Remote Telemetry Unit-ek duen ahultasun bat argitaratu da. Hori baliatuz erasotzaile batek kodea exekuta lezake urrunetik, informazio sentikorra zabaldu, edo zerbitzuaren ukapena eragin.

Xehetasuna:

- Programak ez du neutralizatzen edo oker neutralizatzen du erabiltzailearen sarrera kontrolagarria, beste erabiltzaile batzuei ematen zaien web orrialde bezala erabili baino lehen. Ahultasun horretarako CVE-2020-10630 identifikatzailea erabili da.
- Bereziki diseinatutako eskaera bat baliatuz, erasotzaile batek kaltetutako gailuaren fitxategien egitura ikus lezake, eta irisgarriak izan behar ez luketen fitxategietara sarbidea lortu. Ahultasun horretarako CVE-2020-10634 identifikatzailea erabili da.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Ahultasuna

Kontrolatu gabeko bilaketa bidearen elementua Fazecast-en jSerialComm-en

Argitalpen data: 2020/05/06

Garrantzia: Altua

Kaltetutako baliabideak:

- jSerialComm, 2.2.2 eta lehenagoko bertsioak;
- Schneider Electricen EcoStruxure IT Gateway, 1.5.x, 1.6.x eta 1.7.x bertsioak.

Azalpena:

Securifera-ko Ryan Wincey ikertzaileak, Trend Microko ZDErekin lankidetzan, Fazecast jSerialComm-ek duen larritasun altuko ahultasun baten berri eman dio CISAri, kontrolatu gabeko bilaketa bidearen elementu erakoa.

Konponbidea:

- Fazecast-ek gomendatzen du jSerialComm 2.3 edo geroagoko bertsioetara eguneratzea;
- Schneider Electricek gomendatzen du EcoStruxure IT Gateway 1.8.1 edo geroagoko bertsioetara eguneratzea.

Xehetasuna:

Aurkitutako ahultasuna baliatuz, autentifikatu gabeko urruneko erasotzaile batek kode arbitrarioaren exekuzioa egin lezake xede sisteman, *software*-aren instalazioan existitzen den edozein DLLren izen berdina duen asmo gaiztoko DLL fitxategi bat erabiliz. Ahultasun horretarako CVE-2020-10626 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Pribilegioen kudeaketa desegokia Codesys V3 produktuetan

Argitalpen data: 2020/05/07

Garrantzia: Ertaina

Kaltetutako baliabideak:

- V3.5.16.0 baino lehenagoko CODESYS V3 garapen sistemaren bertsio guztiak, bai 32 eta bai 64 bitetarakoak;
- Ondoko produktuak, V3.5.16.0 bertsioa baino lehenagokoetan:
  - BeagleBone-rako CODESYS Control,
  - emPC-A/iMX6rako CODESYS Control,
  - IOT2000rako CODESYS Control,
  - Linuxerako CODESYS Control,
  - PLCnext-erako CODESYS Control,
  - PFC100erako CODESYS Control,
  - PFC200erako CODESYS Control,
  - Raspberry Pi-rako CODESYS Control,
  - RTE V3rako CODESYS Control,
  - CODESYS Control RTE V3 (Beckhoff CXerako),
  - CODESYS Control Win V3 (CODESYS Development System-en konfigurazioaren zati gisa);
  - CODESYS HMI V3,
  - CODESYS Control V3 Runtime System Toolkit.

Azalpena:

CODESYS V3 garapen sistemak duen pribilegioen kudeaketa desegoki erako ahultasun bat argitaratu da. Hori baliatuz, erasotzaile batek pribilegioen eskalatzea egin lezake.

Konponbidea:

Kaltetutako produktu guztien kasuan, V3.5.16.0 bertsiora eguneratzea.

Xehetasuna:

CODESYSek hainbat aldagai eskaintzen ditu, pantailen bistaratzea erakusteko erabil daitezkeenak. Erabiltzaileen kudeaketa funtzioaren bidez posible da operadore batzuei sarbidea murriztea bistaratzearen zati zehatzetara. CODESYS WebVisu eta CODESYS Remote TargetVisu-n posible da pribilegioen eskalatzea gertatzea, eta horrela operadore zehatz batzuentzat soilik diren bistaratze pantailetara sarbidea lor liteke. Eraso hori baldintza jakin batzuetan bakarrik gerta daiteke:

- Deskargatutako bistaratzearen nabigazioa egiten denean bistaratze pantaila guztiak hautatuta eta soilik nabigaziorako elementuak daudenean babestuta erabiltzeen kudeaketagatik.
- Deskargatutako bistaratzeak nabigazioak ezin eskura ditzakeen bistaratze pantailak dituenean. Ahultasunak bistaratze ezaugarriari berari eragiten dionez, CODESYS Control-en exekuzio denboraren produktuak soilik daude eraginda bistaratze ezaugarria erabiltzen bada.

Ahultasun horretarako CVE-2020-12068 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Advantech WebAccess Node-n

Argitalpen data: 2020/05/08

Garrantzia: Kritikoa

Kaltetutako baliabideak:

WebAccess Node, honako bertsioak:

- 8.4.4 eta lehenagokoak,
- 9.0.0.

Azalpena:

Natnael Samson eta Z0mb1E ikertzaileek, Trend Micro-ko ZDIrekin lankidetzan, 8 ahultasunen berri eman diote CISAri, 3 larritasun kritikokoak, 3 altukoak eta 2 ertainekoak. Honako era hauetakoak dira: *array* baten aurkibidearen baliozkotze desegokia, bideetara kontrolatu gabeko sarbide erlatiboa (*relative path traversal*), SQL injekzioa, pilan (*stack)* oinarritutako bufferraren gainezkatzea, memoria dinamikoan (*heap*) bufferraren gainezkatzea, eta mugez kanpoko irakurketa.

Konponbidea:

8.4.4.P0320844 edo 9.0.0.P0320900 bertsioetara eguneratzea ahultasun horiek konpontzeko.

Xehetasuna: .

- Baliozkotze oker erako ahultasun bat baliatuz, erasotzaile batek bereziki diseinatutako informazioa injekta lezake memorian, eta ondoren bertan exekutatu liteke. Ahultasun horretarako CVE-2020-12022 identifikatzailea erreserbatu da.
- Relative path traversal erako hainbat ahultasun baliatuz, autentifikatutako edo pribilegio maila baxuko erabiltzaile batek bereziki diseinatutako fitxategi bat erabil lezake fitxategiak ezabatu edo gainidazteko, aplikazioaren kontroletik kanpo. Ahultasun horietarako CVE-2020-12010 eta CVE-2020-12006 identifikatzaileak erreserbatu dira.
- Sarrera ez dago ondo sanitizatuta, eta erasotzaile batek SQL komandoak injektatzea baimen dezake. Ahultasun horretarako CVE-2020-12014 identifikatzailea erreserbatu da.
- Pilan (stack) nahiz memoria dinamikoan (heap) oinarritutako bufferraren gainezkatze erako hainbat ahultasun daude, erabiltzaileak emandako datuen luzeraren baliozkotze egoki baten faltak eraginda. Hori baliatuz urruneko kodea exekuta liteke. Ahultasun horietarako CVE-2020-12002 eta CVE-2020-10638 identifikatzaileak erreserbatu dira.
- Mugez kanpoko irakurketa erako ahultasun bat baliatuz, baimendu gabeko datuetara sarbidea eskura liteke. Ahultasun horretarako CVE-2020-12018 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Ahultasuna

Ahultasunak Eaton-en Intelligent Power Manager-en

Argitalpen data: 2020/05/11

Garrantzia: Altua

Kaltetutako baliabideak:

Intelligent Power Manager (IPM), 1.67 eta lehenagoko bertsioak.

Azalpena:

Trend Micro ZDIko Sivathmican Sivakumaran-ek larritasun altuko bi ahultasunen berri eman dio Eaton-i, sarrera parametroen baliozkotze oker eta pribilegioen esleitze oker erakoak.

Konponbidea:

Intelligent Power Manager (IPM) 1.68 bertsiora edo berriago batera eguneratzea.

Xehetasuna:

- IPMk ez ditu modu egokian baliozkotzen inportatuak izan diren konfigurazio fitxategien izenak. Urruneko erasotzaile batek komandoak injekta litzake, edo kode arbitrarioa exekuta lezake sisteman, bereziki sortutako fitxategiak bidaliz. Ahultasun horretarako CVE-2020-6651 identifikatzailea erabili da.
- IPMk ahalbidetzen du konfigurazio fitxategiak bidaltzea administratzaile baimenak ez dituzten erabiltzaileei. Erasotzaile lokal batek sistemaren konfigurazioak manipula litzake parametro okerrak dituzten konfigurazio fitxategiak bidaliz. Ahultasun horretarako CVE-2020-6652 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Schneider Electricen produktuetan

Argitalpen data: 2020/05/13

Garrantzia: Altua

Kaltetutako baliabideak:

- GP-Pro EX, 1.00 bertsiotik 4.09.100 bertsiora bitartekoak;
- Vijeo Designer Basic, 1.1 HotFix 16 eta lehenagoko bertsioak;
- Vijeo Designer, 6.2 SP9 eta lehenagoko bertsioak;
- MTN6501-0001 - U.Motion - KNX Server;
- MTN6501-0002 - U.Motion - KNX Server Plus;
- MTN6260-0410 - U.Motion KNX server Plus, Touch 10;
- MTN6260-0415 - U.Motion KNX server Plus, Touch 15;
- MTN6260-0310 - U.Motion KNX Client Touch 10;
- MTN6260-0315 - U.Motion KNX Client Touch 15.

Azalpena:

Hainbat segurtasun ikertzailek Schneider Electrici 4 ahultasunen berri eman diote, bat kritikotasun altukoa eta 3 kritikotasun ertainekoak. Ahultasun horiek era hauetakoak dira: pasahitzen eskakizun ahulak, barneratutako kredentzialak, sarbidearen kontrol desegokia, eta SQL injekzioa.

Konponbidea:

- GP-Pro EX 4.09.120 bertsiora eguneratzea;
- Vijeo Designer Basic eguneratzea 1.1 HotFix 17 bertsiora.Eguneraketa eskuratzeko beharrezkoa da Schneider Electricen laguntza zerbitzuarekin harremanetan jartzea.
- Vijeo Designer-ek hurrengo *service pack*-ean jasoko du eguneraketa;
- U.Motion Servers eta Touch panels gailuak 1.4.2 bertsiora eguneratzea, eta *Erreferentziak* atala kontsultatzea gailu bakoitzari buruzko eguneraketa berezia eskuratzeko.

Xehetasuna:

- Kritikotasun altuko ahultasunak Vijeo Designer eta Designer Basic gailuei eragiten die. Urruneko erasotzaile batek barneratutako kredentzialak erabil litzake proiektuan edo firmwarean aldaketak egiteko. Ahultasun horretarako CVE-2020-7501 identifikatzailea erreserbatu da.
- Kritikotasun ertaineko ahultasunetarako honako identifikatzaileak erreserbatu dira: CVE-2020-7492, CVE-2020-7492 eta CVE-2020-7500.

Etiketak: Eguneraketa, Schneider Electric, Ahultasuna

Siemensen 2020ko maiatzeko segurtasun buletina

Argitalpen data: 2020/05/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Siemens Power Meters Series 9410, V2.2.1 baino lehenagoko bertsio guztiak;
- Siemens Power Meters Series 9810, bertsio guztiak.

Azalpena:

Siemensek hainbat produkturi buruzko segurtasun eguneraketa batzuk argitaratu ditu bere hileroko komunikatuan.

Konponbidea:

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

Xehetasuna:

Siemensek, segurtasun partxeei buruzko bere hileko komunikatuan 7 segurtasun ohartarazpen argitaratu ditu, horietatik 6 eguneraketak.

Argitaratutako ahultasun mota berriak honako hauek dira:

- Sarbidearen kontrol desegoki erako ahultasun bat,
- osokoen gainezkatze erako 2 ahultasun,
- pilan oinarritutako bufferraren gainezkatze erako ahultasun bat,
- lasterketaren egoera erako 3 ahultasun,
- sistemaren egoeraren kudeaketa desegoki erako ahultasun bat,
- negozioaren logikako akats erako 2 ahultasun.

Ahultasun horietarako honako identifikatzaileak erreserbatu dira: CVE-2019-10938, CVE-2019-12255, CVE-2019-12256, CVE-2019-12258, CVE-2019-12259, CVE-2019-12260, CVE-2019-12261, CVE-2019-12262, CVE-2019-12263 eta CVE-2019-12265.

Etiketak: Eguneraketa, Siemens, Ahultasuna

Hainbat ahultasun OSIsoft PI System-en

Argitalpen data: 2020/05/13

Garrantzia: Altua

Kaltetutako baliabideak:

- PI Asset Framework (AF) Client erabiltzen duten aplikazioak, PI AF Client 2018 SP3 Patch 1 bertsioa eta lehenagokoak erabiltzen dituztenak, 2.10.7.283 bertsioa;
- PI Software Development Kit (SDK) erabiltzen duten aplikazioak, PI SDK 2018 SP1 bertsioa eta lehenagokoak erabiltzen dituztenak, 1.4.7.602 bertsioa;
- Windows Integrated Security-rako PI API, 2.0.2.5 bertsioa eta lehenagokoak;
- PI API, 1.6.8.26 bertsioa eta lehenagokoak;
- PI Buffer Subsystem, 4.8.0.18 bertsioa eta lehenagokoak;
- BACnet-erako PI Connector, 1.2.0.6 bertsioa eta lehenagokoak;
- CygNet-erako PI Connector, 1.4.0.17 bertsioa eta lehenagokoak;
- DC Systems RTscada-rako PI Connector, 1.2.0.42 bertsioa eta lehenagokoak;
- Ethernet/IPrako PI Connector, 1.1.0.10 bertsioa eta lehenagokoak;
- HART-IP-rako PI Connector, 1.3.0.1 bertsioa eta lehenagokoak;
- Ping-erako PI Connector, 1.0.0.54 bertsioa eta lehenagokoak;
- Wonderware Historian-erako PI Connector, 1.5.0.88 bertsioa eta lehenagokoak;
- PI Connector Relay, 2.5.19.0 bertsioa eta lehenagokoak;
- PI Data Archive, PI Data Archive 2018 SP3 bertsioa eta lehenagokoak, 3.4.430.460 bertsioa;
- PI Data Collection Manager, 2.5.19.0 bertsioa eta lehenagokoak;
- Business Analytics-erako PI Integrator, 2018 R2 SP1 bertsioa eta lehenagokoak, 2.2.0.183 bertsioa;
- PI Interface Configuration Utility (ICU), 1.5.0.7 bertsioa eta lehenagokoak;
- PI to OCS, 1.1.36.0 bertsioa eta lehenagokoak;
- PI Vision, 2019 bertsioa eta lehenagokoak;
- PI Manual Logger, 2017 R2 Patch 1 bertsioa eta lehenagokoak;
- RtReports, 4.1 bertsioa eta lehenagokoak.

Azalpena: .

Applied Risk-eko William Knowles segurtasun aholkulari seniorrak, OSIsoft-ekin lankidetzan, 10 ahultasunen berri eman dio CISAri, 5 larritasun altukoak eta 5 ertainekoak. Aurkitutako ahultasun motak honako hauek dira: kontrolatu gabeko bilaketa bideko elementua, sinadura kriptografikoaren egiaztapen okerra, lehenetsitako baimen okerrak, atzeman gabeko salbuespena, erakusle nuluaren deserreferentzia, sarreraren baliozkotze okerra, XSS, eta erregistroko fitxategian informazio konfidentziala jasotzea.

Konponbidea:

Ahultasun bakoitzaren segurtasun neurri zehatzak eskuratzeko irakurri CISAren oharra.

Xehetasuna:

- Erasotzaile lokal batek bilaketa bide bat alda dezake eta bitar bat erabili ekipo lokalaren kontrola hartzeko Windows sistemaren pribilegio mailan. Ondorioz, baimendu gabeko informazioa hedatu, ezabatu edo alda liteke. Ahultasun horretarako CVE-2020-10610 identifikatzailea erreserbatu da.
- Erasotzaile lokal batek bitar bat erabil dezake eta kodearen integritatearen egiaztapena saihestu, PI System-en liburutegiak kargatzeko. Horrela baimendu gabeko informazioa hedatu, ezabatu edo alda lezake. Ahultasun horretarako CVE-2020-10608 identifikatzailea erreserbatu da.
- Kaltetutako produktuak ezarritako baimen okerrak balia litzake erasotzaile lokal batek. Ahultasun hau baliatuz baimendu gabeko informazioa hedatu, ezabatu edo alda liteke, ekipo lokalak beste erabiltzaile batzuen PI System datuak ere prozesatzen baditu. Ahultasun horretarako CVE-2020-10606 identifikatzailea erreserbatu da.
- Autentifikatu gabeko urruneko erasotzaile batek PI Network Manager-en zerbitzua blokea lezake bereziki diseinatutako eskaeren bidez. Horrek PI Data Archive-rako konexioak eta kontsultak blokea litzake. Ahultasun horretarako CVE-2020-10604 identifikatzailea erreserbatu da.
- Autentifikatutako urruneko erasotzaile batek PI Network Manager blokea lezake lasterketako baldintza baten ondorioz. Horrek PI

Data Archive-rako konexioak eta kontsultak blokea litzake. Ahultasun horretarako CVE-2020-10602 identifikatzailea erreserbatu da.
- Autentifikatutako urruneko erasotzaile batek PI Archive Subsystem blokea lezake azpisistemak memoriaren presio pean funtzionatzen duenean. Egoera horrek PI Data Archive-rako kontsulten blokeoa eragin lezake. Ahultasun horretarako CVE-2020-10600 identifikatzailea erreserbatu da.
- Autentifikatutako urruneko erasotzaile batek objektuaren barne ezaugarriak gehitu edo alda litzake, eta ondorioz zehaztugabeko portaera gertatuko litzateke. Ahultasun horretarako CVE-2019-10768 eta CVE-2019-11358 identifikatzaileak erabili dira.
- Autentifikatutako urruneko erasotzaile batek bereziki diseinatutako URLak erabil litzake, PI Vision mugikorra erabiltzen ari den erabiltzaile bat webgune ahul batera bidaltzeko, hirugarrenen osagai batean dagoen arazo baten ondorioz. Ahultasun horretarako CVE-2020-10600 identifikatzailea erreserbatu da.
- Autentifikatutako urruneko erasotzaile batek, PI Vision-en datu baseetara idazketa sarbidea izanez gero, kodea injekta lezake pantailan, eta horrela baimendu gabeko informazioa hedatu, ezabatu edo aldatu lezake erabiltzaile batek kaltetutako pantaila erabiliz gero. Ahultasun horretarako CVE-2020-10614 identifikatzailea erreserbatu da.
- Erasotzaile lokal batek informazio konfidentziala kontsulta lezake erregistro fitxategietan, zerbitzu kontuak pertsonalizatzen direnean PI Vision-en instalazioan edo eguneraketan. Ahultasun horretarako CVE-2019-18244 identifikatzailea erabili da.

Etiketak: Ahultasuna

Sarbidearen kontrol desegoki erako ahultasuna Emersonen WirelessHART Gateways-en

Argitalpen data: 2020/05/15

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Ondoko zerrendako produktuak ahultasuna daukate VLAN ezaugarria gaituta daukatenean:

- Wireless 1410 Gateway, 4.6.43 bertsiotik 4.7.84 bertsiora bitartekoak;
- Wireless 1420 Gateway, 4.6.43 bertsiotik 4.7.84 bertsiora bitartekoak;
- Wireless 1552WU Gateway, 4.6.43 bertsiotik 4.7.84 bertsiora bitartekoak.

Azalpena:

Emersonek larritasun kritikoko ahultasun bat aurkitu du, sarbidearen kontrol desegoki erakoa.

Konponbidea:

Emersonek gomendatzen du VLAN ezaugarriaren 4 bertsioa gaituta duten produktu kaltetuak eskuragarri dagoen firmwarearen azken bertsiora eguneratzea.

Xehetasuna:

Lotura ateko barne firewall-a konfiguratzeko erabiltzen den kodeak duen akats batek, VLAN ezaugarria gaituta dagoenean, firewall hori desgaitu egiten du, gailuak erabiltzen dituen ataka guztiak agerian utziz. Urruneko erasotzaile batek ahultasun hori balia lezake erabiltzaileen haririk gabeko gailuetan ekintzak egiteko. Ahultasun horretarako CVE-2020-12030 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Azpiegitura kritikoak, Ahultasuna

---

Hainbat ahultasun Opto 22ren SoftPAC Project-en

Argitalpen data: 2020/05/15

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Opto 22 SoftPAC Project, 9.6 eta lehenagoko bertsioak.

Azalpena:

Claroty-ko Mashav Sapir-ek 5 ahultasunen berri eman dio CISAri, 2 larritasun kritikokoak eta beste 3 ertainekoak. Honako era hauetakoak dira: fitxategi izenaren edo bidearen kanpo kontrola, sinadura kriptografikoaren egiaztapen okerra, sarbidearen kontrol okerra, kontrolatu gabeko bilaketa bidearen elementua, eta baimentze okerra.

Konponbidea:

Ahultasun horiek konpontzeko Opto 22-k PAC Project-en 10.3 bertsioa argitaratu du, PAC Project Professional eta PAC Project Basic-erako eskuragarri dagoena.

Xehetasuna:

- SoftPAC-en *firmware*-a eguneratzeko erabiltzen diren zip fitxategien barnean zehazten diren bideak ez dira sanitizatzen. Ondorioz, erabiltzaile pribilegioak dituen erasotzaile batek sarbide arbitrarioa eskura lezake sistemarako sarbidea duten fitxategietan idazteko. Ahultasun horretarako CVE-2020-12042 identifikatzailea erabili da.
- SoftPAC-en *firmware*-aren fitxategietako sinadurak ez dira egiaztatzen *firmware* horren eguneraketarekin. Hori baliatuz erasotzaile batek firmware fitxategi zilegizkoak ordezka litzake asmo gaiztoko fitxategiekin. Ahultasun horretarako CVE-2020-12046 identifikatzailea erabili da.
- 22000 ataka murrizpenik gabe dago irekita. Hori baliatuz sarera sarbidea lukeen erasotzaile batek SoftPACAgent zerbitzua kontrola lezake, SoftPACAgent-en *firmware*-aren eguneraketa barne, zerbitzua abiarazi edo gelditu lezake, edo erregistroko balio jakin batzuetan idatzi. Ahultasun horretarako CVE-2020-10612 identifikatzailea erabili da.
- Erasotzaile batek DLL fitxategiak ordezka litzake eta kodea exekutatu SoftPAC zerbitzua abiatzen den bakoitzean, fitxategi horietako hainbatetan inportazio bidea ez baita zehazten. Ahultasun horretarako CVE-2020-10616 identifikatzailea erabili da.
- Sarera sarbidea lukeen erasotzaile bat zuzenean komunikatu liteke SoftPAC-ekin, PLC honek ez baitu inolako kredentzial motarik bere komunikazioetan. Ahultasun horretarako CVE-2020-10620 identifikatzailea erabili da.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Ahultasuna

Hainbat ahultasun Emersonen OpenEnterprise SCADA Softwaren

Argitalpen data: 2020/05/2020

Garrantzia: Kritikoa

Kaltetutako baliabideak:

OpenEnterprise SCADA Software, 3.3.4 eta lehenagoko bertsioak.

Azalpena:

Kaspersky-ko Roman Lozkok larritasun kritiko, altu eta ertaineko hiru ahultasunen berri eman dio Emersoni. Honako era hauetakoak dira hurrenez hurren: funtzio kritikorako autentifikazio falta, fitxategien ezaugarriaren kudeaketa okerra, eta zifratuaren sendotasun desegokia.

Konponbidea:

Emersonek bere erabiltzaile guztiei gomendatzen die OpenEnterprise 3.3 Service Pack 5 (3.3.5) bertsiora eguneratzea, Emerson SupportNet plataforman eskuragarri.

Xehetasuna:

- Kaltetutako osagaiak baliatuz, erasotzaile batek komando arbitrarioak exekuta litzake sistemaren pribilegioekin, edo kodearen urruneko exekuzioa egin lezake komunikazio zerbitzu zehatz baten bitartez. Ahultasun horretarako CVE-2020-10640 identifikatzailea erreserbatu da.
- Karpetaren segurtasun baimen desegokiak baliatuz, konfigurazio fitxategi garrantzitsuak alda litezke, eta horrek eragin lezake sistemak huts egitea edo ustekabeko moduan funtzionatzea. Ahultasun horretarako CVE-2020-10632 identifikatzailea erreserbatu da.
- Zifratu desegokia baliatuz OpenEnterprise-ren erabiltzaile kontuetarako pasahitzak eskura litezke. Ahultasun horretarako CVE-2020-10636 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Azpiegitura kritikoak, SCADA, Ahultasuna

Informazio konfidentziala testu lauan gordetzen da Sensormatic Electronics-en hainbat produktutan

Argitalpen data: 2020/05/22

Garrantzia: Kritikoa

Recursos afectados:

- Software House C?CURE 9000, versión 2.70;
- American Dynamics victor Video Management System, versión 5.2.
- Software House C-CURE 9000, 2.70 bertsioa;
- American Dynamics victor Video Management System, 5.2 bertsioa.

Azalpena:

Johnson Controls-ek larritasun kritikoko ahultasun baten berri eman dio CISAri, informazio konfidentziala testu lauan gordetzearen erakoa. Johnson Controls-ena den Sensormatic Electronics LLC enpresaren hainbat produkturi eragiten die.

Konponbidea:

- Software House C-CURE 9000: 2.80 edo bertsio berriagoetara eguneratzea;
- American Dynamics victor Video Management System: 5.3 bertsiora eguneratzea;
- Erregistro fitxategiak ezabatu *c:/programdata/tyco/installertemp*-etik eta Windowseko kontuaren pasahitza aldatzea.

Xehetasuna:

C-CURE 9000ren 2.70 bertsioaren eta American Dynamics victor Video Management System-en 5.2 bertsioaren instalazioan edo eguneratzean, instalazioa edo eguneratzea egiten duten erabiltzailearen kredentzialak fitxategi batean gordetzen dira. Instalazioaren erregistro fitxategiak iraun egiten du instalazioaren ondoren ere. Ahultasun horretarako CVE-2020-9045 identifikatzailea erabili da.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Osasuna, Ahultasuna

Ahultasuna ABBren Device Library Wizard-en

Argitalpen data: 2020/05/22

Garrantzia: Altua

Kaltetutako baliabideak:

ABB Device Library Wizard, 6.0.X, 6.0.3.1 eta 6.0.3.2 bertsioak.

Azalpena:

ABBren Device Library Wizard-ek duen ahultasun bat argitaratu da, informazioaren hedapen erakoa. Hori baliatuz erasotzaile batek sistemaren nodo baten edo gehiagoren kontrola har lezake.

Konponbidea:

-
- 6.0.3.2 RU1, 6.0.3.3, 6.1.X edo geroagoko bertsioetara eguneratzea.
- Era berean, ABBk gomendatzen du esperientziarik ez duten pertsonek ezagutu litzaketen erabiltzaile kontuen pasahitzak aldatzea. Gomendatzen da sarbide interaktiboa (bai lokala eta bai urrunekoa) desgaitzea artikulu hauen zerbitzu konturako.

Xehetasuna:

Device Library Wizard-en kaltetutako bertsioek datu konfidentzialak dituen fitxategi bat sortzen dute, pribilegio gutxiko erabiltzaileek irakur lezaketena. Hori baliatuz erasotzaile batek sistemaren nodo bat edo gehiagoren kontrola har lezake. Ahultasun horretarako CVE-2020-8482 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Sarbidearen kontrol desegoki erako ahultasuna Kantech EntraPass-en

Argitalpen data: 2020/05/27

Garrantzia: Altua

Kaltetutako baliabideak:

Kantech EntraPass Special Edition, Corporate Edition eta Global Edition, 8.22 eta lehenagoko bertsioak.

Azalpena:

Johnson Controls-ek sarbidearen kontrol desegoki erako larritasun altuko ahultasun baten berri eman dio CISAri, Johnson Controls enpresarena den Kantech-en EntraPass produktuaren hainbat bertsiori eragiten diena.

Konponbidea:

Johnson Controls-ek gomendatzen du Kantech EntraPass edizio guztiak 8.23 bertsiora eguneratzea.

Xehetasuna:

Kantech EntraPass-ek daukan ahultasun bat baliatuz, pribilegio gutxiko erabiltzaile baimendu batek pribilegio guztiak eskura litzake sistema mailan, fitxategi kritikoak bereziki diseinatutako fitxategiekin ordezkatzean. Ahultasun horretarako CVE-2020-9046 identifikatzailea erabili da.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Ahultasuna

Hainbat ahultasun Bosch Recording Station-en

Argitalpen data: 2020/05/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Bosch Recording Station.

Azalpena:

Bosch Recording Station (BRS) produktuan 4 ahultasun aurkitu dira, bi kritikoak, bat altua eta bat ertaina. Era honetakoak dira: kodearen urruneko exekuzioa, sarbidearen kontrol desegokia eta datu konfidentzialen zifratze falta.

Konponbidea:

Bosch Recording Station eguneratzea DIVAR IP *all-in-one* 5000-era.

Xehetasuna:

- Bosch Recording Station-i BlueKeep ahultasunak eragiten dio, Windows 7 erabiltzearen ondorioz.Ahultasun horretarako CVE-2019-0708 identifikatzailea erabili da.
- Bosch Recording Station-en *Kiosk Mode* funtzionaltasunak duen sarbidearen kontrol okerra baliatuz, autentifikatu gabeko erasotzaile lokal bat *Kiosk Mode*-tik irten liteke, eta azpiko sistema eragilera sarbidea lortu. Ahultasun horretarako CVE-2020-6774 identifikatzailea erabili da.
- Bosch Recording Station-i EternalBlue ahultasunak eragiten dio, Windows 7 erabiltzearen ondorioz.Ahultasun horretarako CVE-2017-0144 identifikatzailea erabili da.
- Bosch Recording Station ez da bateragarria Full Disk Encryption-ekin. Sistemara sarbide fisikoa lukeen erasotzaile batek sistemaren unitatea fisikoki ezaba lezake, eta fitxategien sistemaren edukia irakurri eta aldatu.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

SWARCO TRAFFIC SYSTEMS markako CPU

LS4000 sisteman sarbide desegokia egiteko arriskua

Argitalpen data: 2020/05/29

Garrantzia: Kritikoa

Kaltetutako baliabideak:

CPU LS4000, G4rekin hasitako sistema eragilearen bertsio guztiak.

Deskripzioa:

ProtectEM enpresako Martin Aman ikertzaileak, taldeak koordinatuta, ahultasun kritiko bat atzeman du CPU LS4000 produktuan, eta SWARCO TRAFFIC SYSTEMS etxeari horren berri eman dio.

Konponbidea:

SWARCO TRAFFIC SYSTEMS markak partxe bat sortu zuen ahultasuna zuzendu eta portua ixteko. SWARCO TRAFFIC SYSTEMS erakundeko harremanetarako pertsonak informazio gehiago eman dezake.

Xehetasuna:

Depuraziorako erabilitako portu ireki batek aukera ematen du gailura root sarbidea egiteko, sarearen bidezko sarbidea kontrolatu gabe. Erasotzaile batek ahultasun hori baliatu lezake gailura sartu ahal izateko eta konektatutako gailuekin eragiketak alteratzeko. Ahultasun horretarako, CVE-2020-12493 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.