2019ko Ekainaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Autentifikazioari ihes egitea Ewon-en web zerbitzarian

Argitalpen data: 2019/06/04

Garrantzia: Handia

Kaltetutako baliabideak:

- Fabrikatzailearen gailu guztiak, 12.2 bertsiotik 13.0ra bitarteko *firmwareren* bat badute.

Azalpena:

Howest-eko (UGent) Tijl Deneut segurtasun ikertzaileak autentifikazioaren ihes erako ahultasun honen berri eman du. Ahultasun hau arrakastaz baliatuz gero, erasotzaile batek informazio sentikorraren irakurketak egin litzake.

Konponbidea:

- Fabrikatzaileak gomendatzen du kaltetutako *firmware* bertsioak 13.1s0 bertsiora eguneratzea.

Xehetasuna:

- Kaltetutako gailuen web zerbitzuan autentifikatu gabe dagoen erasotzaile batek autentifikazioa saihets lezake, eta horrela informazio sentikorrera sarbidea lortuko luke. Ahultasun honek ez die eragiten Talk2M soluzioa erabiltzen duten erabiltzaileei. Soilik eragingo lieke Ewon-en erabiltzaile lokalei.

Etiketak: Eguneraketa, Ahultasuna

Autentifikazioaren eta sarbideen kontrolaren kudeaketa okerra Tecson/GOK produktuetan

Argitalpen data: 2019/06/05

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- LX-Net
- LX-Q-Net
- e-litro net
- SmartBox4 LAN
- SmartBox4 pro LAN

Azalpena:

Maxim Rupp (rupp.it) ikertzaileak Tecson/GOK produktuek duten ahultasun baten berri eman du, sarbideen kontrola eta autentifikazioa kudeatzeko moduari eragiten diona.

Konponbidea:

- Gailuen *firmwarea* 6.3.x bertsioa baino berriago batera eguneratzea

Xehetasuna:

- Aplikazioak ez ditu modu egokian kudeatzen web baliabideetarako sarbideak, eta hainbat baliabidetarako sarbidea ahalbidetzen du

autentifikazioaren beharrik gabe. Ahultasun hori baliatuz urruneko erasotzaile batek web zerbitzariaren bide zehatzetan (URL) kokatutako baliabideetara sarbidea lor lezake, autentifikatuta egon behar izan gabe. Baliabide horietarako sarbide zuzenak web zerbitzaria osorik kontrolatzea ahalbidetzen du, eta horrela konfigurazioan eta gailuen ezarpenetan, adibidez pasahitz, parametro edo alertetan, aldaketak egin daitezke. Ahultasun horretarako CVE-2019-12254 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun ABBren gailuetan

Argitalpen data: 2019/06/05

Garrantzia: Handia

Kaltetutako baliabideak:

- Ondoren zerrendatzen diren produktuen G1 berrikusketa indizea, BSP UN31rekin, 1.76 bertsioa eta lehenagokoak:
  - CP620 y CP620-WEB
  - CP630 y CP630-WEB
  - CP635, CP635-B y CP635-WEB
- 1.91tik 2.8.0.367ra bitarteko bertsioak, honako produktuarena:
  - PB610 Panel Builder 600
- Ondoren zerrendatzen diren produktuen B1 berrikusketa indizea, BSP UN30ekin, 1.76 bertsioa eta lehenagokoak:
  - CP651
  - CP661
  - CP665
  - CP676
- Ondoren zerrendatzen diren produktuen A0 berrikusketa indizea, BSP UN30ekin, 1.76 bertsioa eta lehenagokoak:
  - CP651-WEB
  - CP661-WEB
  - CP665-WEB
  - CP676-WEB

Azalpena:

ABBk Xen1thLabs, Darkmatter Company, United Arab Emirates eta Abu Dhabi-ri eskertu die informazioa eman eta kontzeptu probak egin izana ahultasun mota hauei buruz: eguneratu gabeko softwarearen osagaiak, barneratutako kredentzialak, sinaduraren egiaztapen eza, ezkutuko administratzaile kontuak, direktorio jauzia FTP zerbitzarian, FTP eta HTTP zerbitzarietara bidalitako kateen formatuan kontrolik eza, pilan oinarritutako bufferraren gainezkatzea, eta web zerbitzarian autentifikazioa saihestea. Urruneko erasotzaile batek kode arbitrarioa exekuta lezake eta ahultasunek kaltetutako gailuetan funtzionamendu okerra eragin lezake, haiek arrakastaz baliatuz gero.

Konponbidea:

Fabrikatzaileak erabiltzaileen eskura jarri ditu honako eguneraketa hauek:

- PB610 Panel Builder 600, V2.8.0.424
- BSP UN31 V2.31
- BSP UN30 V2.31

Xehetasuna:

- ABB CP635 HMI eta CP651 HMI gailuak:
  - Kodean barneratutako administrazio kontu bat daukate, eta hori HDMIren ezarpenaren fasean erabiltzen da. 'Panel Builder 600' konfigurazio tresnara sarbidea lukeen erasotzaile batek kredentzial horiek erabil litzake HMIan interfaze berriak sortzeko edo HMIan mapeatzen diren balioen etiketak (MODBUS coils) aldatzeko. Ahultasun horretarako CVE-2019-7225 identifikatzailea erreserbatu da.
  - Gailuak eguneratzean fitxategien transmisioak duen zifratze falta dela eta, eguneraketen egiaztapena eguneraketa paketearen eta azken transmisioaren artean egiten da, fitxategi bitarren hashak alderatzearen bidez. Sarera edo eguneraketa paketera sarbidea lukeen erasotzaile batek fitxategi bitar horiek manipula litzake, gailua osorik arriskuan jarriz. Ahultasun horretarako CVE-2019-7229 identifikatzailea erreserbatu da.
  - Gailuek eguneratu gabe dauden eta ahulak diren software osagaiak dituzte, firmwarearen fitxategietan eta zerbitzu bitarretan estatikoki estekatuta daudenak.
- ABB PB610:
  - Kodean barneratutako administrazio kontu bat dauka, eta hori HDMIren ezarpenaren fasean erabiltzen da. 'Panel Builder 600' konfigurazio tresnara sarbidea lukeen erasotzaile batek kredentzial horiek erabil litzake HMIan interfaze berriak sortzeko edo HMIan mapeatzen diren balioen etiketak (MODBUS coils) aldatzeko. Ahultasun horretarako CVE-2019-7225 identifikatzailea erreserbatu da
  - IDAL HTTP CGI zerbitzariak URL bat eskuragarri dauka eta hori baliatuz erasotzaile batek autentifikazioa saihets dezake eta funtzioetara sarbidea lortu pribilegio altuekin. Ahultasun horretarako CVE-2019-7226 identifikatzailea erreserbatu da.
  - IDAL FTP zerbitzariak ez ditu modu egokian kudeatzen direktorio aldaketako eskariak. Hori baliatuz erasotzaile batek fitxategien edozein bidetara sarbidea lor lezake, FTP zerbitzariaren ingurunetik kanpo. Ahultasun horretarako CVE-2019-7227 identifikatzailea erreserbatu da.
  - IDAL HTTP eta IDAL FTP zerbitzariek ez dituzte zuzen baliozkotzen erabiltzaileen sarrerak. Hori baliatuz erasotzaile batek memoria honda lezake gaizki sortutako sarrerekin, autentifikazioa saihesteko edo urrunetik kodea exekutatzeko. Ahultasun horietarako CVE-2019-7228 eta CVE-2019-7230 identifikatzaileak erreserbatu dira.
  - HTTP zerbitzariak bufferraren gainezkatze erako ahultasuna dauka. Urruneko erasotzaile batek HTTP eskaeraren goiburuko host eremua alda dezake bufferraren gainezkatzea eragiteko, eta horrela Structure Exception Handler-aren (SEH) helbidea gainidatzi buffer handiago batekin.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Hainbat ahultasun Geutebrück-en produktuetan

Argitalpen data: 2019/06/05

Garrantzia: Handia

Kaltetutako baliabideak:

Ahultasunek Encoder eta E2 Series Camera-ren ondoko bertsio eta modeloei eragiten diete:

- G-Code: 1.12.0.25 bertsio guztiak eta lehenagokoak.
  - EEC-2XXX
- G-Cam: 1.12.0.25 bertsio guztiak eta lehenagokoak.
  - EBC-21XX
  - EFD-22XX
  - ETHC-22XX
  - EWPC-22XX

Azalpena:

Romain Luyer eta CEISeko Guillaume Gronnier ikertzaileek, RandoriSec-eko Davy Douhine-rekin batera, Cross-site Scripting (XSS) eta sistema operatiboko komandoen injekzio erako hainbat ahultasunen berri eman dute. Ahultasun horiek arrakastaz baliatuz gero urruneko erasotzaile batek urruneko kodea exekuta lezake root modura eta kodea exekutatu IP kameraren operadorearen nabigatzailean.

Konponbidea:

- Fabrikatzaileak erabiltzaile erregistratuentzat ahultasun horiek arintzen dituen firmwarearen eguneraketa bat argitaratu du:
  - 1.12.13.2 bertsioa

Xehetasuna:

- Gertaeren konfiguraziora sarbidea lukeen autentifikatutako urruneko erasotzaile batek asmo gaiztoko kodea gorde lezake zerbitzarian. Hori ondoren erabiltzaile legitimo batek exekuta lezake, eta orduan erabiltzailearen nabigatzailearen barnean kodea exekutatuko litzateke. Ahultasun horretarako CVE-2019-10957 identifikatzailea erreserbatu da.
- Autentifikatutako urruneko erasotzaile batek komandoak exekuta litzake root modura, bereziki diseinatutako URL komando baten bidez. Ahultasun horretarako CVE-2019-10956 identifikatzailea erreserbatu da.
- Erabiltzailearen sarrera parametroetan dagoen baliozkotze oker bat baliatuz, sarearen konfiguraziora sarbidea lukeen urruneko erasotzaile batek sistemaren komandoak sar litzake zerbitzarian, eta horrela urruneko kodea exekutatzea lortuko luke root modura. Ahultasun horretarako CVE-2019-10958 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Gemalto-ren Sentinel LDKn

Argitalpen data: 2019/06/06

Garrantzia: Txikia

Kaltetutako baliabideak:

- Sentinel LDK, 7.92 bertsioaren aurreko guztiak

Azalpena:

Kaspersky Lab-eko Artem Zinenko ikertzaileak Gemalto-ren Sentinel LDKri eragiten dioten «HTTPOnly» atributurik gabeko cookie erako eta komunikazioak testu argian erako hainbat ahultasunen berri eman du. Urruneko erasotzaile batek man-in-the-middle erako eraso bat egin lezake, eta biktimaren hizkuntzaren paketea ordeztu edo erabiltzailearen cookiea lapurtu.

Konponbidea:

- Ahultasun horiek konpontzeko Sentinel LDK 7.92 bertsiora eguneratzea gomendatzen da.

Xehetasuna:

- *«HTTPOnly» atributurik gabeko cookiea: «Hasplm» cookieak «HTTPOnly» atributurik ez dauka. Hori baliatuz erasotzaile batek cookiea lapurtu lezake javascript kodearen bidez. Ahultasun horretarako CVE-2019-8283 identifikatzailea erreserbatu da.*
- Komunikazioak testu argian: Gemalto Admin Control Center softwareak HTTP testu argiko komunikazioak erabiltzen ditu www3.safenet-inc.com-ekin komunikatzeko, hizkuntza paketeak eskuratzearren. Hori baliatuz erasotzaile batek man-in-the-middle erako eraso bat egin lezake, eta hizkuntzaren paketea ordeztu asmo gaiztoko beste batekin. Ahultasun horretarako CVE-2019-8282 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Panasonic-en Control FPWINen

Argitalpen data: 2019/06/07

Garrantzia: Handia

Kaltetutako baliabideak:

- FPWIN Pro, 7.3.0.0 eta lehenagoko bertsioak.

Azalpena:

9sg Security Team-eko kimiya ikertzaileak, Trend Micro-ko Zero Day Initiative-rekin lankidetzan, Panasonic-en PLC Control FPWIN Pro-ren programazio softwareari eragiten dioten bufferraren gainezkatze erako eta baliabideetara sarbide erako ahultasun batzuen berri eman du. Ahultasun horiek arrakastaz baliatuz gero, erasotzaile batek gailua gera lezake eta kodea exekutatu urrunetik.

Konponbidea:

- Ahultasun horiek konpontzeko Panasonic-ek erabiltzaileei gomendatzen die FPWIN Pro 7.3.1.0 bertsiora edo berriago batera eguneratzea.

Xehetasuna:

- Erasotzaile batek sortu eta autentifikatutako erabiltzaile batek kargatzen dituen proiektu fitxategiek bufferraren gainezkatzea eragin lezakete. Horren ondorioz kodea exekuta liteke urrunetik. Ahultasun horretarako CVE-2019-6530 identifikatzailea erreserbatu da.
- Fitxategi horiek beraiek sarbide akatsak eragin litzakete bateraezin motako baliabideetara (type confusion) baliabideak ez dituelako espero diren ezaugarriak. Horren ondorioz kodea exekuta liteke urrunetik. Ahultasun horretarako CVE-2019-6532 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Optergy-ren Proton Enterprise Building Management System-en

Argitalpen data: 2019/06/07

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Proton Enterprise, 2.3.0 eta lehenagoko bertsioak.

Azalpena:

Applied Risk-eko Gjoko Krstic ikertzaileak Optergy-ren Proton Enterprise-ri eragiten dioten hainbat ahultasunen berri eman du: informazioaren hedapena, gune gurutzatuetan eskaeraren faltsutzeak (CSRF), fitxategi arriskutsuen murrizpenik gabeko igoera, asmo gaiztoko URLetara birbideratzea, ezkutuko funtzionaltasuna, metodo edo funtzio arriskutsua agerian uztea eta softwarean barneratutako kredentzialak. Horiek baliatuz erasotzaile batek kodea exekuta lezake urrunetik, sistemaren informazioa zabaldu eta sisteman sarbide osoa eskuratu.

Konponbidea:

- Fabrikatzaileak gomendatzen duen konponbidea da Optergy zerbitzariak 2.4.5 bertsiora eguneratzea.

Xehetasuna:

- Aplikazioaren erabiltzaile izena berrezartzeko funtzionaltasunaren bidez, erasotzaileak sisteman baliagarriak diren erabiltzaile guztiak zerrendatu eta agerian utz litzake, eta gainera sistemaren barneko informazioa zabal lezake. Ahultasun horietarako CVE-2019-7272 eta CVE-2019-7277 identifikatzaileak erabili dira.
- Kargaren unean fitxategien luzapena baliozkotzen ez denez, autentifikaziorik gabeko urruneko erasotzaile batek baliozkotu gabeko luzapenak dituzten fitxategiak karga litzake, eta igoak izan diren direktorioaren barnean exekutatu. Ahultasun horretarako CVE-2019-7274 identifikatzailea erabili da.
- Identifikatu gabeko backdoor baten bidez, erasotzaile batek sistemarako sarbidea eskura lezake eta kode arbitrarioa exekutatu. Ahultasun horretarako CVE-2019-7276 identifikatzailea erabili da.
- Autentifikatu gabeko erabiltzaileek aitortu gabeko klaseen funtzioak erabil litzakete zenbait baliabidetara sarbidea lortzeko. Ahultasun horretarako CVE-2019-7278 identifikatzailea erabili da.
- Erasotzaile batek softwarean barneratutako kredentzialak erabil litzake baimendu gabeko SMS mezuak bidaltzeko edozein telefono zenbakitara. Ahultasun horretarako CVE-2019-7279 identifikatzailea erabili da.
- Gainerako ahultasunetarako honako identifikatzaileak esleitu dira: CVE-2019-7273 eta CVE-2019-7275.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Siemens produktuetan

Argitalpen data: 2019/06/11

Garrantzia: Handia

Kaltetutako baliabideak:

- Siveillance VMS 2017 R2, 11.2a baino lehenagoko bertsio guztiak
- Siveillance VMS 2018 R1, 12.1a baino lehenagoko bertsio guztiak
- Siveillance VMS 2018 R2, 12.2a baino lehenagoko bertsio guztiak
- Siveillance VMS 2018 R3, 12.3a baino lehenagoko bertsio guztiak
- Siveillance VMS 2019 R1, 13.1a baino lehenagoko bertsio guztiak
- SCALANCE X-200, 5.2.4 bertsioa baino lehenagoko guztiak
- SCALANCE X-200IRT, SCALANCE X-300 y SCALANCE X-414-3E, bertsio guztiak
- SIEMENS LOGO!8
  - 6ED1052-xyyxx-0BA8, FS:01etik FS:06ra bitartekoak / Firmwarearen V1.80.xx eta V1.81.xx bertsioak
  - 6ED1052-xyy08-0BA0 FS:01 / firmwarearen V1.82.02 bertsioa baino lehenagokoak
- SIMATIC Ident MV420 eta MV440 familiak

Azalpena:

Siemens-en CERTek eta cirosec GmbH, Ruhr University of Bochum, Hochschule Augsburg eta Pen Test Partners-eko ikertzaileek Siemensen zenbait produkturi eragiten dieten hainbat ahultasun aurkitu dituzte.

Konponbidea:

- Siveillance VMS 2017 R2, 11.2a bertsiora eguneratu
- Siveillance VMS 2018 R1, 12.1a bertsiora eguneratu
- Siveillance VMS 2018 R2, 12.2a bertsiora eguneratu
- Siveillance VMS 2018 R3, 12.3a bertsiora eguneratu
- Siveillance VMS 2019 R1, 13.1a bertsiora eguneratu
- SCALANCE X-200, 5.2.4 bertsiora eguneratu

Kaltetutako gainerako produktuen kasuan, ahultasunak arintzeko Siemensek gomendatzen du honako ekintza hauek egitea:

- 80/TCP atala blokatzea kanpoko suebakian.
- Gailuetan gordetako backup konfigurazioetara edo konfigurazio fitxategietara sarbidea murriztea.
- Gailuen konfigurazioetara sare bitartez sartzeko mekanismoak murriztea edo desgaitzea, gaituta dauden kasuetan.
- C-PLUG konfigurazio modulurako sarbidea murriztea, erabilgarri dagoen kasuetan.
- Kaltetutako produktuetara sartzea ahalbidetzen duen sarea babestea.
- DISA bit-a konfiguratzean, erabiltzaile erregistratuek proiektuan aldaketak egitea ekiditea. Funtzionamendurako argibideak kontsultatzea.

Xehetasuna:

Argitaratutako ahultasun motak honako hauek dira:

- Autentifikazio gabezia. Ahultasun horretarako CVE-2019-6581 eta CVE-2019-6582 identifikatzaileak erreserbatu dira.
- Pasahitzak ateratzea. Ahultasun horretarako CVE-2019-6567 identifikatzailea erreserbatu da.
- Zerbitzuaren ukapena. Ahultasun horretarako CVE-2019-6571 identifikatzailea erreserbatu da.
- Saio hasierako IDak eskuratzea. Ahultasun horretarako CVE-2019-6584 identifikatzailea erreserbatu da.
- Pribilegioen eskalatzea. Ahultasun horretarako CVE-2019-10925 identifikatzailea erreserbatu da.
- Informazioa zabaltzea. Ahultasun horretarako CVE-2019-10926 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Siemens, Ahultasuna

Fitxategien kudeaketa okerra DICOM estandarrean

Argitalpen data: 2019/06/12

Garrantzia: Handia

Kaltetutako baliabideak:

- NEMA DICOM estandarrarekin (.dcm luzapena) fitxategiak kudeatzen dituzten gailu eta software produktu guztiak, 1995tik 2019b-ra bitarteko bertsioak.

Azalpena:

Cylera Labs-eko Markel Picado Ortiz (d00rt) ikertzaileak DICOM (Digital Imaging and Communications in Medicine) estandarrak fitxategiak kudeatzean duen ahultasun baten berri eman du. Ahultasun hori baliatuz erasotzaile batek DICOM *.dcm motako osasun irudien fitxategiak alda litzake asmo gaiztoko kodea txertatzeko.

Konponbidea:

- Osasun irudien sistema guztietan antibirus soluzio bat ezartzea gomendatzen da, bai eta DICOM Security Group-ek argitaratutako txosten batean adierazitako gomendioak jarraitzea ere.

Xehetasuna:

- Ahultasuna balia liteke kode exekutagarria txertatuz DICOM motako fitxategi baten goiburuaren parte den 128 byteko atarikoan. Erasotzaile batek aldatu egin lezake goiburu ezberdin bat kapsulatzeko. Aldatutako fitxategi berri hori baliatuz, erasotzaileak asmo gaiztoko kodea txertatu eta exekuta lezake *.dcm luzapena duten osasun irudien DICOM motako fitxategietan. Ahultasun horretarako CVE-2019-11687 identifikatzailea erabili da.

Etiketak: Ahultasuna

Hainbat ahultasun Schneider Electric-en produktuetan

Argitalpen data: 2019/06/12

Garrantzia: Handia

Kaltetutako baliabideak:

- PowerSCADA Expert 7.30
- PowerSCADA Expert 7.40
- PowerSCADA Expert 8.0, Service Release 1 gabe
- ProClima, 8.0.0 baino lehenagoko bertsio guztiak

Azalpena:

NSFOCUSen segurtasun ekipoko ikertzaileek era ezberdinetako ahultasunak aurkitu dituzte: kodearen injekzioa, buffer akatsak, kontrolatu gabeko bilaketa bidea, eta informazio sentikorra agerian uztea. Horiek baliatuz informazio sentikorra eskura liteke eta urruneko kodea exekutatu.

Konponbidea:

Firmwarea eguneratzea:

- ProClima 8.0.0 bertsiora edo berriagora.
- PowerSCADA 9.0 bertsiora edo berriagora.

Xehetasuna:

- Kodearen injekzioaren bidez autentifikaziorik gabeko urruneko erasotzaile batek kode arbitrarioa exekuta lezake xede den sisteman. Ahultasun horretarako CVE-2019-6823 identifikatzailea erreserbatu da.
- Buffer akats bati esker autentifikaziorik gabeko urruneko erasotzaile batek kode arbitrarioa exekuta lezake xede den sisteman.

Ahultasun horretarako CVE-2019-6824 identifikatzailea erreserbatu da.
- Kontrolatu gabeko bilaketaren path elementuak duen ahultasuna baliatuz, asmo gaiztoko DLL fitxategi batek kode arbitrarioa exekuta lezake instalazio softwarearen barneko edozein DLLren izen berdinarekin. Ahultasun horretarako CVE-2019-6825 identifikatzailea erreserbatu da.
- Ahultasun bat baliatuz autentifikatutako erabiltzaile lokal batek Citect-en erabiltzailearen kredentzialetara sarbidea lor lezake. Ahultasun horretarako CVE-2019-10981 identifikatzailea erabili da.

Etiketak: Eguneraketa, SCADA, Schneider Electric, Ahultasuna

Hainbat ahultasun WAGO 852 Industrial Managed Switch-en

Argitalpen data: 2019/06/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- 852-303, v1.2.2.S0 baino lehenagoko bertsioak
- 852-1305, v1.1.6.S0 baino lehenagoko bertsioak
- 852-1505, v1.1.5.S0 baino lehenagoko bertsioak

Azalpena:

SEC Consult Vulnerability Lab-eko T. Weber ikertzaileak hainbat ahultasun aurkitu ditu WAGO 852 switch industrialetan. Horien arrazoia da barneratutako firmware-ak ahulak diren liburutegiak eta software osagaiak erabiltzen dituela. Ahultasun horiek baliatuz erasotzaile batek gailura sartzea lor lezake firmwarean barneratutako kredentzialei eta gako pribatuei esker. Era berean bufferraren gainezkatzea balia lezake, eta kaltetutako gailuetan ezegonkortasuna eragin.

Konponbidea:

Fabrikatzaileak erabiltzaileei gomendatzen die beren switcha eguneratzea eskuragarri dagoen firmwarearen azken bertsioarekin.

- 852-303: 1.2.2.S0 bertsioa edo berriagoa.
- 852-1305: 1.1.6.S0 bertsioa edo berriagoa.
- 852-1505: 1.1.5.S0 bertsioa edo berriagoa.

Xehetasuna:

- Kodetutako kredentzialetara sarbidea lukeen erasotzaile batek switcharen sistema eragilera sarbidea lortuko luke root pribilegioekin. Horri esker switcharen sistema eragilea manipula lezake. Ahultasun horretarako CVE-2019-12550 identifikatzailea erreserbatu da.
- Kodetutako SSH gakora sarbidea lukeen erasotzaile batek komunikazioa eten lezake edo switcha arriskuan jarri. Erabiltzaileek ezin dituzte SSH gakoak berrezarri eta switch guztiek gako berdina erabiltzen dute. Ahultasun horretarako CVE-2019-12549 identifikatzailea erreserbatu da.
- Hirugarrenen osagai ahulak: zerrendatutako produktuek ahultasun ezagunak dituzten hirugarrenen software osagaiak erabiltzen dituzte. Horiek arrakastaz baliatuz gero urruneko erasotzaile batek switcha arriskuan jar lezake edo bertan zerbitzuaren ukapen egoera eragin. Ahultasun horietako batzuen identifikatzaileak ondokoak dira, erabilitako liburutegi ahul bakoitzerako:
  - BusyBox 1.12.0: CVE-2013-1813, CVE-2016-2148, CVE-2016-6301, CVE-2011-2716, CVE-2011-5325, CVE-2015-9261, CVE-2016-2147, CVE-2017-16544 etc.
  - GNU glibc 2.8: CVE-2010-0296, CVE-2010-3856, CVE-2012-4412, CVE-2014-4043, CVE-2014-9402, CVE-2014-9761, CVE-2014-9984, CVE-2015-14 etc.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Eguneraketa desegokia Johnson Controls-en ESMn

Argitalpen data: 2019/06/14

Garrantzia: Ertaina

Kaltetutako baliabideak:

exacqVision ESM, 5.12.2 bertsioa eta lehenagokoak, Windows sistema guztietan Windows Server-en izan ezik.

Azalpena:

@bzyo_ ikertzaileak baimentze desegoki erako ahultasun bat aurkitu du Johnson Controls-en exacqVision ESM produktuetan. Ahultasun hori arrakastaz baliatuz gero, asmo gaiztoko kodea exekuta liteke sisteman.

Konponbidea:

Produktua 19.03 bertsiora eguneratzea.

Xehetasuna:

Modu lehenetsian, sisteman pribilegio gutxi dituzten baimendutako kontuen direktorioei gehiegizko baimenak ematen zaizkie. Erasotzaile batek hori balia lezake instalatutako aplikazioen fitxategietan aldaketak egiteko edo pribilegioak eskalatzeko. Ahultasun horretarako CVE-2019-7588 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun BDren (Becton, Dickinson and Company) Alaris Gateway Workstation-en

Argitalpen data: 2019/06/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Alaris Gateway Workstation, 1.0.13, 1.1.3 Build 10, 1.1.3 MR Build 11, 1.1.5, 1.1.6, 1.2 Build 15 eta 1.3.0 Build 14 bertsioak.
- Modu osagarrian, ondoko produktuak ere bai, 2.3.6 bertsioan eta lehenagokoetan:
  - Alaris GH.
  - Alaris CC.
  - Alaris TIVA.

Azalpena:

CyberMDXko Elad Luz ikertzaileak hainbat ahultasun aurkitu ditu BDren (Becton, Dickinson and Company) Alaris Gateway Workstation-en. Horiek baliatuz sarera sarbidea lukeen urruneko erasotzaile batek gailuko informazio sentikorra bistaratu lezake, konfigurazioak editatu, urruneko kodea exekutatu edo zerbitzuaren ukapen egoera eragin.

Konponbidea:

- Alaris Gateway Workstation-ek duen ahultasunaren kasuan:
  - Azken firmwarera eguneratzea, 1.3.2 edo 1.6.1 bertsioa.
  - Kaltetutako produktua dagoen sarera erabiltzaileek egiten dituzten sarbideak kontrolatzea.
  - Kaltetutako produktua duten sistemak isolatzea zilegi ez diren sistemen aurrean.
- Alaris Gateway lan estazioko fitxategi arriskutsuen kargaren ahultasunaren kasuan:
  - SMB protokoloa blokatzea.
  - Sarea bereiztea VLANen erabilerarekin.
  - Sarerako sarbidea erabiltzaile baimenduek soilik dutela ziurtatzea.

Xehetasuna:

- Alaris Gateway Workstation-ek eskaintzen duen nabigazio interfazeak ez ditu modu zuzenean kudeatzen informazio sentikorra duten fitxategi ezberdinetarako sarbideak. Alaris-en IPa ezagutuko lukeen erasotzaile batek ahultasun hori balia lezake gailu horretako konfigurazioei buruzko informazioa eskuratzeko. Ahultasun horretarako CVE-2019-10962 identifikatzailea erabili da.
- Aplikazioak ez du firmware eguneraketa batean gailura igo daitezkeen fitxategien murrizpen egokirik. Ahultasun hori baliatuz erasotzaile batek asmo gaiztoko edukia duten fitxategiak igo litzake. Ahultasun horretarako CVE-2019-10959 identifikatzailea erabili da.

Etiketak: Ahultasuna

Bufferraren gainezkatze erako ahultasuna Advantech-en WebAccess-en

Argitalpen data: 2019/06/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

WebAccess/SCADA 8.4.0,bertsioa. .

Azalpena:

WebAccess/SCADA softwareari eragiten dioten bufferraren gainezkatze erako bi ahultasunen berri eman dioTenable-k Advantech-i. Ahultasun horiek baliatuz autentifikaziorik gabeko urruneko erasotzaile batek kodea exekuta lezake modu arbitrarioan.

Konponbidea:

WebAccess/SCADA 8.4.1 bertsiora edo berriagoetara eguneratzea.

Xehetasuna:

- viewsrv.dll-k ahultasun bat dauka, eta horren arrazoia da erabiltzaileak emandako datuen baliozkotze okerra, datuak tamaina finkoko pilaren buffer batera kopiatu aurretik, IOCTL 10012 RPC dei bat prozesatzen denean. Ahultasun horretarako CVE-2019-3953 identifikatzailea erabili da.
- viewdll1.dll-eko VdBroadWinGetLocalDataLogEx() funtzioak ahultasun bat dauka, eta horren arrazoia da erabiltzaileak emandako datuen baliozkotze okerra, datuak tamaina finkoko pilaren buffer batera kopiatu aurretik, RPC IOCTL 81024 mezu bat prozesatzen denean.Ahultasun horretarako CVE-2019-3954 identifikatzailea erabili da.

Etiketak: Eguneraketa, SCADA, Ahultasuna

Hainbat ahultasun Phoenix Contact-en Automation Worx Software Suite-n

Argitalpen data: 2019/06/20

Garrantzia: Handia

Kaltetutako baliabideak:

Automationworx Software Suite-ren osagaiak, 1.86 bertsioa eta lehenagokoak:

- PC Worx
- PC Worx Express
- Config

Azalpena:

9sg Security Team-ek jakinarazi duenez, Phoenix Contact-en Automationworx-en produktuek hainbat eratako ahultasunak dituzte: hasieratu gabeko erakusle bitartezko kodearen urruneko exekuzioa, memoria erabili ondoren bere askapenaren bitartezko kodearen urruneko exekuzioa, eta mugez kanpoko irakurketagatiko informazioaren hedapena.

Konponbidea:

Ahultasun hori Automationworx Software Suite-ren hurrengo bertsioan zuzenduko da.

Xehetasuna:

PC Worx edo Config-en proiektu fitxategi batera sarbidea duen erasotzaile batek hori manipulatzen badu eta aplikazioen programaziorako lan estazioan trukatzen badu, kode arbitrarioa exekuta lezake urrunetik. Ahultasun horietarako CVE-2019-12869, CVE-2019-12870 eta CVE-2019-12871 identifikatzaileak erreserbatu dira.

Etiketak: 0day, Ahultasuna

Kredentzial barneratuak SICK-en MSC800-en

Argitalpen data: 2019/06/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

MSC800, 4.0 baino lehenagoko bertsioak

Azalpena:

Amazon-eko Customer Fulfillment Technology Security (CFTS) taldeko Tri Quach-ek kredentzial barneratuen erako ahultasun baten berri eman du.

Konponbidea:

MSC800 gailua 4.0 edo goragoko bertsio batera eguneratzea.

Xehetasuna:

Kaltetutako firmware bertsioek bezero kontuaren pasahitz bat daukate barneratuta. Ahultasun hori arrakastaz baliatuz gero, autentifikaziorik gabeko urruneko erasotzaile batek gailuaren konfigurazioak alda litzake edota bere funtzionamendua eten. Ahultasun horretarako CVE-2019-10979 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Advantech-en WebAccess-en

Argitalpen data: 2019/06/28

Garrantzia: Kritikoa

Azalpena:

SCADA WebAccess-ek dituen hainbat eratako ahultasunak argitaratu dira: direktorioen arteko jauzia, bufferraren gainezkatzea, mugez kanpoko irakurketa, mugez kanpoko idazketa, eta fidagarria ez den erakuslearen deserreferentzia. Horiek baliatuz, informazio konfidentziala hedatu, fitxategiak ezabatu edo urruneko kodea exekuta liteke.

Konponbidea:

WebAccess 8.4.1 bertsiora eguneratzea.

Xehetasuna:

- Direktorioen arteko jauzi erako ahultasun bat dago, erabiltzaileak sartutako bide batean falta den baliozkotze batek eraginda, fitxategien eragiketara aplikatua izan aurretik. Hori baliatuz, erasotzaile batek fitxategiak ezabatu litzake administratzaile baimenekin. Ahultasun horretarako CVE-2019-10985 identifikatzailea erabili da.
- Pilaren bufferraren gainezkatze erako hainbat ahultasun daude, erabiltzaileak sartutako datuen luzera ez egiaztatzeak eraginda. Hori baliatuz erasotzaile batek urruneko kodea exekuta lezake. Ahultasun horretarako CVE-2019-10991 identifikatzailea erabili da.
- Memoria dinamikoan bufferraren gainezkatze erako hainbat ahultasun daude, erabiltzaileak sartutako datuen luzera ez egiaztatzeak eraginda. Hori baliatuz erasotzaile batek urruneko kodea exekuta lezake. Ahultasun horretarako CVE-2019-10989 identifikatzailea erabili da.
- Erabiltzaileak sartutako datuak egiaztatzen ez direnez, erasotzaile batek informazioa ezagutzera eman lezake. Ahultasun horretarako CVE-2019-10983 identifikatzailea erabili da.
- Erabiltzaileak sartutako datuen luzera ez egiaztatzearen ondorioz, urruneko kodea exekuta liteke. Ahultasun horretarako CVE-2019-10987 identifikatzailea erabili da.
- Fidagarria ez den erakuslearen deserreferentzia erako ahultasun bat baliatuz, urruneko erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2019-10993 identifikatzailea erabili da.

Etiketak: Eguneraketa, SCADA, Ahultasuna

Sarbidearen kontrol okerra Medtronic-en MiniMed intsulina ponpetan

Argitalpen data: 2019/06/28

Garrantzia: Handia

Kaltetutako baliabideak:

- MiniMed 508, bertsio guztiak;
- MiniMed Paradigm 511511, bertsio guztiak;
- MiniMed Paradigm 512/712, bertsio guztiak;
- MiniMed Paradigm 712E, bertsio guztiak;
- MiniMed Paradigm 515/715, bertsio guztiak;
- MiniMed Paradigm 522/722, bertsio guztiak;
- MiniMed Paradigm 522K/722K, bertsio guztiak;
- MiniMed Paradigm 523/723, 2.4A edo lehenagoko bertsioak;
- MiniMed Paradigm 523K/723K, 2.4A edo lehenagoko bertsioak;
- MiniMed Paradigm Veo 554/754, 2.6A edo lehenagoko bertsioak;
- MiniMed Paradigm Veo 554CM eta 754CM, 2.7A edo lehenagoko bertsioak.

Azalpena:

Nathanael Paul, Jay Radcliffe, Barnaby Jack, Billy Rios, Jonathan Butts eta Jesse Young ikertzaile independenteek kritikotasun altuko ahultasun hau aurkitu dute. Ahultasun hau arrakastaz baliatuz gero, erasotzaile batek intsulina ponparen konfigurazioak alda litzake edo horietan eragin, edo ponparen administrazioa kontrolatu.

Konponbidea:

Medtronic-ek oraindik ez du arindu ahultasun hau, baina kaltetutako pazienteei gomendatzen die beren intsulina ponpa berriago batengatik eguneratzea.

Xehetasuna:

Kaltetutako intsulina ponpak beste gailu batzuekin komunikatzen dira, adibidez glukometroekin, haririk gabeko RF komunikazio bat erabiliz, eta horrek ez du modu zuzenean inplementatzen autentifikazioa edo baimentzea. Sarbide eremuaren barnean legokeen erasotzaile batek kaltetutako ponpa modeloetara sartzea lor lezake eta ezarritako dosiak aldatu, baita datuak atzeman ere. Ahultasun horretarako CVE-2019-10964 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna