2019ko Abuztuaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Hainbat ahultasun Rockwell Automation-en Arena Simulation Software-n

Argitalpen data: 2019/08/02

Garrantzia: Handia

Kaltetutako baliabideak:

Arena Simulation Software for Manufacturing, Cat. 9502-Ax, 16.00.00 eta lehenagoko bertsioak.

Azalpena:

9SG Security Team-eko kimiya ikertzaileak, Zero Day Initiative-rekin (ZDI) lankidetzan, askatu ondoreneko memoriaren erabilpen erako eta informazioa agerian uztearen erako hainbat ahultasunen berri eman du, Rockwell Automation-en Arena Simulation Software-ri eragiten diotenak. Ahultasun horiek arrakastaz baliatuz gero, erasotzaile batek akatsa eragin lezake saioan, eta horrela zerbitzuaren ukapen egoera (DoS) eragin edo kode arbitrarioa exekutatu.

Konponbidea:

Ahultasun horiek konpontzeko Rockwell Automation-ek Arena Simulation Software-ren 16.00.01 bertsioa argitaratu du.

Xehetasuna:

- Bereziki diseinatutako Arena fitxategi bat erabiltzaile batek irekiz gero, aplikazioan akats bat eragin lezake edo kode arbitrarioa exekutatu liteke. Ahultasun horretarako CVE-2019-13510 identifikatzailea erreserbatu da.
- Bereziki diseinatutako Arena fitxategi bat erabiltzaile batek irekiz gero, erasoaren biktima den lan estazioarekin zerikusia duen informazio mugatua agerian utz liteke. Ahultasun horretarako CVE-2019-13511 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Mugez kanpoko irakurketa Advantech-en WebAccess HMI Designer-en

Argitalpen data: 2019/08/02

Garrantzia: Handia

Kaltetutako baliabideak:

Advantech WebAccess HMI Designer, 2.1.9.23 eta lehenagoko bertsioak.

Azalpena:

Zero Day Initiative-ko (ZDI) Mat Powell-ek mugez kanpoko irakurketa erako ahultasun baten berri eman du, Advantech-en WebAccess HMI Designer softwareari eragiten diona. Ahultasun hori arrakastaz baliatuz gero, urruneko erasotzaile batek kode arbitrarioa exekuta lezake.

Konponbidea:

Advantech-ek ahultasun horiek konpontzen dituen WebAccess HMI Designer-en 2.1.9.31 bertsioa argitaratu du.

Xehetasuna:

Bereziki diseinatutako MCR fitxategiak prozesatzerakoan erabiltzaileak emandako datuen baliozkotze desegoki bat dela eta,

aurreikusitako bufferraren areatik kanpo idatz lezake sistemak, eta horren ondorioz kodea exekuta liteke urrunetik. Ahultasun horretarako CVE-2019-10961 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Mugez kanpoko irakurketa Fuji Electric-en FRENIC Loader-en

Argitalpen data: 2019/08/02

Garrantzia: Txikia

Kaltetutako baliabideak:

FRENIC Loader, 3.5.0.0 eta lehenagoko bertsioak.

Azalpena:

9SG Security Team-eko Kimiya-k, Zero Day Initiative-rekin (ZDI) lankidetzan, mugez kanpoko irakurketa erako ahultasun baten berri eman du, Fuji Electric-en FRENIC Loader-i eragiten diona. Ahultasun hau arrakastaz baliatuz gero, erasotzaile batek informazioa zabal lezake.

Konponbidea:

Fuji Electric-ek ahultasun hori konpontzen duen FRENIC Loader-en bertsio berri bat argitaratu du.

Xehetasuna:

Kaltetutako produktua ahula da mugez kanpoko irakurketa baten aurrean. Hori baliatuz, erasotzaile batek gailuko informazio mugatua irakur lezake. Ahultasun horretarako CVE-2019-13512 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun EZAutomation-en produktuetan

Argitalpen data: 2019/08/13

Garrantzia: Handia

Kaltetutako baliabideak:

- EZTouch Editor.
- EZPLC.

Azalpena:

9sg Security Team-eko ekipoak bufferraren gainezkatze erako eta fitxategien analisian gertatutako memoriaren hondatze erako hainbat ahultasunen berri eman du. Horiek baliatuz urruneko erasotzaile batek kode arbitrarioa exekuta lezake EZTouch Editor eta EZPLCren instalazio ahuletan.

Konponbidea:

Ahultasunaren izaera kontuan izanik, arintze estrategia bakarra aplikazioarekiko interakzioa murriztea da.

Xehetasuna:

- Erabiltzaileak EZC fitxategietan emandako datuen baliozkotze okerrak memoriaren hondatze egoera sortzen du. Hori baliatuz urruneko erasotzaile batek kodea exekuta lezake oraingo prozesuaren testuinguruan EZPLC produktuaren instalazioetan. Beste erabiltzaile baten interakzioa beharrezkoa da, asmo gaiztoko orrialde batera sar dadin edo asmo gaiztoko fitxategi bat ireki dezan.
- EZC fitxategietan, erabiltzaileak emandako datuak bufferrean kopiatu baino lehen horien tamainaren baliozkotze okerra baliatuz, urruneko erasotzaile batek kodea exekuta lezake oraingo prozesuaren testuinguruan EZTouch Editor produktuaren instalazioetan. Beste erabiltzaile baten interakzioa beharrezkoa da, asmo gaiztoko orrialde batera sar dadin edo asmo gaiztoko fitxategi bat ireki dezan.

Etiketak: 0day, Ahultasuna

Hainbat ahultasun Siemens produktuetan

Argitalpen data: 2019/08/13

Garrantzia: Handia

Kaltetutako baliabideak:

- SCALANCE X-200, bertsio guztiak.
- SCALANCE X-200IRT, bertsio guztiak.
- SCALANCE X-200RNA, bertsio guztiak.
- SIMATIC ET 200SP Open Controller CPU 1515SP PC, bertsio guztiak.
- SIMATIC ET 200SP Open Controller CPU 1515SP PC2, bertsio guztiak.
- SIMATIC S7-1200 familia CPU, bertsio guztiak.
- SIMATIC S7-1500 familia CPU, V4.0 bertsioa baino goragoko guztiak.
- SIMATIC S7-1500 Software Controller, bertsio guztiak.

- SIMATIC S7-PLCSIM Advanced, bertsio guztiak.
- SINAMICS GH150 V4.7 (Control Unit), bertsio guztiak.
- SINAMICS GH150 V4.8 (Control Unit), V4.8 SP2 HF6 baino lehenagoko bertsio guztiak.
- SINAMICS GL150 V4.7 (Control Unit), bertsio guztiak.
- SINAMICS GL150 V4.8 (Control Unit), V4.8 SP2 HF7 baino lehenagoko bertsio guztiak.
- SINAMICS GM150 V4.7 (Control Unit), bertsio guztiak.
- SINAMICS GM150 V4.8 (Control Unit), V4.8 SP2 HF9 baino lehenagoko bertsio guztiak.
- SINAMICS SL150 V4.7 (Control Unit), bertsio guztiak.
- SINAMICS SL150 V4.8 (Control Unit), bertsio guztiak.
- SINAMICS SM120 V4.7 (Control Unit), bertsio guztiak.
- SINAMICS SM120 V4.8 (Control Unit), bertsio guztiak.
- SCALANCE SC-600, V2.0 bertsioa.
- SCALANCE XB-200, V4.1 bertsioa.
- SCALANCE XC-200, V4.1 bertsioa.
- SCALANCE XF-200BA, V4.1 bertsioa.
- SCALANCE XP-200, V4.1 bertsioa.
- SCALANCE XR-300WG, V4.1 bertsioa.

Azalpena:

Zenbait ikertzailek hainbat ahultasunen berri eman dute. Horiek baliatuz gero *man-in-the-middle* (MitM) zerbitzuaren ukapen erako erasoak egin litezke, programaren iturburu kodea aldatu eta komando arbitrarioak exekutatu.

Konponbidea:

Siemensek hainbat eguneraketa garatu ditu kaltetutako gailuentzat.

Xehetasuna:

- Gailuak daukan ahultasun bat baliatuz erasotzaile batek zerbitzuaren ukapen egoera sor lezake, Telnet zerbitzura behin eta berriz mezuen pakete handiak bidaliz. Ahultasun horretarako CVE-2019-10942 identifikatzailea erreserbatu da.
- Kaltetutako gailuen web zerbitzariak duen ahultasun bat baliatuz, erasotzaile batek zerbitzuaren ukapen egoera sor lezake eta kaltetutako gailuaren web zerbitzariaren berrabiatzea eragin. Ahultasun horretarako CVE-2019-6568 identifikatzailea erabili da.

Larritasun ertain eta baxuko gainerako ahultasunetarako ondoko identifikatzaileak erreserbatu dira: CVE-2019-10929, CVE-2019-10943, CVE-2019-10927 eta CVE-2019-10928.

Etiketak: Eguneraketa, Komunikazioak, Siemens, Ahultasuna

Hainbat ahultasun OSIsoft PI Web APIan

Argitalpen data: 2019/08/14

Garrantzia: Handia

Kaltetutako baliabideak:

OSIsoft PI Web API, 2018 bertsioa eta lehenagokoak.

Azalpena:

OSIsoftek bi eratako ahultasunak aurkitu ditu, bat *log* fitxategietako informazio sentikorraren inklusio erakoa eta bestea CSRF erasoen aurkako babes mekanismoen akats erakoa.

Konponbidea:

Ahultasun horiek zuzentzeko OSIsoft-ek erabiltzaileei gomendatzen die PI Web API 2018 SP1 bertsiora edo geroagoko batera eguneratzea.

Xehetasuna:

- OSIsoft PI Web aplikazioak sortutako log fitxategiek gertakari batzuen aurrean informazio sentikorra agerian uzten dute. Hori erasotzaile batek balia dezake eraso sofistikatuagoak egiteko. Ahultasun horretarako CVE-2019-13515 identifikatzailea erreserbatu da.
- Aplikazioan ezarritako CSRF (*Cross-Site Request Forgery*) erako erasoen aurkako babes mekanismoak ez dira eraginkorrak bertsio ahulean. Ahultasun horretarako CVE-2019-13516 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Delta Industrial Automation DOPSoft-en

Argitalpen data: 2019/08/14

Garrantzia: Handia

Kaltetutako baliabideak:

- DOPSoft, 4.00.06.15 eta lehenagoko bertsioak.

Azalpena:

9SG Security Team-eko Kimiya ikertzaileak mugez kanpoko irakurketa erako eta aldez aurretik askatutako memoriaren kokapenen erabilpen erako hainbat ahultasunen berri eman du. Horiek baliatuz informazioa heda liteke, kodea urrunetik exekutatu edo aplikazioaren akatsa eragin.

Konponbidea:

Delta Electronics-ek kaltetutako erabiltzaileei gomendatzen die 4.00.06.47 edo geroagoko bertsio batera eguneratzea, bai eta aplikazioarekiko interakzioa fitxategi fidagarrietara murriztea.

Xehetasuna:

- Bereziki diseinatutako proiektuaren fitxategi baten prozesaketak aldez aurretik askatutako memoriaren erabilpen erako edo mugez kanpoko irakurketa erako hainbat ahultasun eragin litzake. Horren ondorioz informazioa heda liteke, urruneko kodea exekutatu edo aplikazioan akatsa eragin. Ahultasun horietarako CVE-2019-13514 eta CVE-2019-13513 kodeak esleitu dira.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Schneider Electric produktuetan

Argitalpen data: 2019/08/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Magelis HMIGTO series, bertsio guztiak.
- Magelis HMISTO series, bertsio guztiak.
- Magelis XBTGH series, bertsio guztiak.
- Magelis HMIGTU series, bertsio guztiak.
- Magelis HMIGTUX series, bertsio guztiak.
- Magelis HMISCU series, bertsio guztiak.
- Magelis HMISTU series, bertsio guztiak.
- Magelis XBTGT series, bertsio guztiak.
- Magelis XBTGC series, bertsio guztiak.
- Magelis HMIGXO series, bertsio guztiak.
- Magelis HMIGXU series, bertsio guztiak.
- Modicon M340 kontrolatzailea, bertsio guztiak.
- BMXNOR0200H Ethernet / Serial RTU modulua, bertsio guztiak.
- SoMachine HVAC, 2.4.1 eta lehenagoko bertsioak.
- 2019/07/15 baino lehen fabrikatutako TelevisGo.
- Schneider Electric Software Update (SESU) - SUT Service osagaia, 2.1.1 bertsiotik 2.3.0ra bitartekoak.
- spaceLYnk, 2.4.0 baino lehenagoko bertsio guztiak.
- KNXerako (homeLYnk) Wiser, 2.4.0 baino lehenagoko bertsio guztiak.

Azalpena:

Hainbat ikertzailek era ezberdinetako ahultasunen berri eman dute: ohiz kanpoko baldintzen kudeaketa desegokia, sarbide kontrol desegokia, baliabideen bilaketarako direktorioaren gaineko kontrola, memoriaren bufferraren murrizpen desegokia, baliabideen kudeaketa desegokia, mugez kanpoko irakurketa eta idazketa, memoriaren bufferraren kudeaketa okerra, baliabideen kudeaketan akatsa, datuen interpretazio okerra eta autentifikazio okerra. Ahultasun horiek baliatuz erasotzaile batek HMIa blokea lezake, zerbitzuaren ukapen egoera eragin, konexio aktiboak deskonektatu, baimenik gabeko erabiltzaile baten partetik komandoak exekutatu, gailuan kode arbitrarioa exekutatu, kodea urrunetik exekutatu, bufferraren memoriaren gainezkatzea eragin eta erasotzaile batek autentifikazioa saihesten duenean kontrola galdu arazi.

Konponbidea:

- EcoStruxure Machine Expert HVAC, 1.1.0 bertsioa.
- TelevisGo, 2019/07/15etik aurrerako bertsioak.Lehenagoko bertsioen kasuan, TelevisGo_HotFix_20190715.exe instalatu.
- SESU - SUT Service, 2.3.1 bertsioa.
- spaceLYnk, *firmware*-aren 2.4.0_HW_1_X_X eta 2.4.0_HW_2_X_X_HW_3_X_X bertsioak.
- KNXrako Wiser, *firmware*-aren 2.4.0_HW_1_X_X eta 2.4.0_HW_2_X_X_HW_3_X_X bertsioak.
- Eguneraketa zehatzik ez duten gainerako produktuen kasuan, arintze neurriak eta praktika onak ezarri.

Xehetasuna:

Ondoren zehazten dira larritasun kritikoko ahultasunak:

- TelevisGO-n barneratutako UltraVNC produktuak memoriaren bufferrean duen eragiketen murrizpen oker bat baliatuz, kaltetutako sisteman dagoen sarera sarbidea lukeen erasotzaile batek urruneko kodea exekuta lezake. Ahultasun horretarako CVE-2019-8258 eta CVE-2018-15361 identifikatzaileak erabili dira.
- TelevisGO-n barneratutako UltraVNC produktuak memoriaren bufferrean duen mugez kanpoko irakurketa bat baliatuz, kaltetutako sisteman dagoen sarera sarbidea lukeen erasotzaile batek informazio sentikorra eskura lezake. Ahultasun horretarako CVE-2019-8260 eta CVE-2019-8261 identifikatzaileak erabili dira.
- TelevisGO-n barneratutako UltraVNC produktuak memoriaren bufferrean duen errore sorta bat baliatuz, kaltetutako sisteman dagoen sarera sarbidea lukeen erasotzaile batek urruneko kodea exekuta lezake. Ahultasun horretarako CVE-2019-8262, CVE-2019-8273, CVE-2019-8274 eta CVE-2019-8271 identifikatzaileak erabili dira.
- TelevisGO-n barneratutako UltraVNC produktuak memoriaren bufferrean duen mugez kanpoko irakurketa eta idazketa baliatuz, kaltetutako sisteman dagoen sarera sarbidea lukeen erasotzaile batek urruneko kodea exekuta lezake. Ahultasun horretarako CVE-2019-8280, CVE-2019-8264, CVE-2019-8265 eta CVE-2019-8266 identifikatzaileak erabili dira.
- TelevisGO-n barneratutako UltraVNC produktuan exekutatutako kalkulu okerrek eragindako bufferraren tamainaren kudeaketa okerra baliatuz, kaltetutako sisteman dagoen sarera sarbidea lukeen erasotzaile batek urruneko kodea exekuta lezake. Ahultasun horretarako CVE-2019-8268 eta CVE-2019-8272 identifikatzaileak erabili dira.
- TelevisGO-n barneratutako UltraVNC produktuak sarbideen kontrolean duen kudeaketa okerra baliatuz, kaltetutako sisteman dagoen sarera sarbidea lukeen erasotzaile batek erabiltzaile bakoitzarentzat ezarritako mugez kanpoko datuak eskura litzake. Ahultasun horretarako CVE-2019-8275 identifikatzailea erabili da.

Larritasun altu eta ertaineko gainerako ahultasunetarako ondoko identifikatzaileak esleitu dira: CVE-2019-8259, CVE-2019-8263, CVE-2019-8267, CVE-2019-8276, CVE-2019-8277, CVE-2019-8269, CVE-2019-8270, CVE-2019-6826, CVE-2019-6813, CVE-2019-6831, CVE-2019-6810, CVE-2019-6813, CVE-2019-6833, CVE-2019-6834 eta CVE-2019-6832.

Etiketak: Eguneraketa, Komunikazioak, Pribatutasuna, Schneider Electric, Ahultasuna

---

Bufferraren gainezkatzea Fuji Electric-en Alpha5 Smart Loader-en

Argitalpen data: 2019/08/16

Garrantzia: Handia

Kaltetutako baliabideak:

- Alpha5 Smart Loader, 4.2 bertsioaren aurreko guztiak.

Azalpena:

Natnael Samson ikertzaileak, Trend Micro's Zero Day Initiative-rekin lankidetzan, bufferraren gainezkatze erako ahultasun baten berri eman du Alpha5 Smart Loader softwarean. Hori baliatuz erasotzaile batek kodea exekuta lezake aplikazioak dituen pribilegio berdinekin.

Konponbidea:

4.2 bertsiora eguneratzea.

Xehetasuna:

Erasotzaile batek proiektuko fitxategia asmo gaiztoz manipula lezake, Alpha5 Smart Loader aplikazioan bufferraren gainezkatzea eragiteko. Horrela kodea exekutatu ahal izango luke aplikazioa exekutatzen ari den pribilegioekin. Ahultasun horretarako CVE-2019-13520 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna

Hainbat ahultasun Johnson Controls-en Metasys building automation sistemetan

Argitalpen data: 2019/08/16

Garrantzia: Ertaina

Kaltetutako baliabideak:

- Metasys building automation automatizazio sistema, 9.0 bertsioa baino lehenagoko guztiak

Azalpena:

harpocrates.ghost ikertzaileak enkriptatze gakoen berrerabilpen eta kodean barneratutako gakoen erako hainbat ahultasunen berri eman du. Horiek baliatuz urruneko erasotzaile batek sareko komunikazioak deszifra litzake, eta horrela horien konfidentzialtasunari eragin.

Konponbidea:

Johnson Controls fabrikatzaileak v9.0 baino geroagoko bertsioetara eguneratzea gomendatzen du eta komunikazioak konfiguratzea konfiantzako ziurtagiriak erabiltzeko.

Xehetasuna:

- Metasys-en ADS/ADX zerbitzariek eta NAE/NIE/NCE motorrek Site Management Portal-en (SMP) aurkako eragiketarako erabilitako hainbat RSA zifratze gako partekatzen dituzte. Partekatutako RSA gako horietara sarbidea lukeen erasotzaile batek komunikazioak deszifra litzake, bai ADS/ADX zerbitzarietakoak eta bai NAE/NIE/NCEtakoak, SMP bezeroaren aurka egindakoak. Ahultasun horretarako CVE-2019-7593 identifikatzailea erabili da.
- Metasys-en ADS/ADX zerbitzariek eta NAE/NIE/NCE motorrek Site Management Portal-en (SMP) aurkako hainbat eragiketetarako barneratutako RSC2 gakoak erabiltzen dituzte. Barneratutako RC2 gako horietara sarbidea lukeen erasotzaile batek komunikazioak deszifra litzake, bai ADS/ADX zerbitzarien artekoak eta bai NAE/NIE/NCE moterretakoak, SMP bezeroaren aurka egindakoak. Ahultasun horretarako CVE-2019-7594 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Bosch-en ProSyst mBS SDK eta IoT Gateway Software-n

Argitalpen data: 2019/08/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- ProSyst mBS SDK, 8.2.6 baino lehenagoko bertsioak;
- Bosch IoT Gateway Software, 9.0.2, 9.2.0 eta 9.3.0 baino lehenagoko bertsioak.

Azalpena:

Kaltetutako produktuetan bide jauzi, Server-Side Request Forgery (SSRF) eta informazioa agerian uztearen erako hainbat ahultasun aurkitu dira. Horiek baliatuz urruneko erasotzaile batek informazio sentikorrera sarbidea lor lezake, sistemako informazioa idatzi eta ezabatu eta zerbitzariaren izenean HTTPren GET eskaera bat bidali.

Konponbidea:

ProSyst mBS SDK eguneratzea 8.2.6 bertsiora eta IoT Gateway 9.3.0 bertsiora.

Xehetasuna:

- *Backup/Restore* funtziorako urruneko sarbideak duen bide jauzi erako ahultasun bat baliatuz, urruneko erasotzaile batek edozein kokagunetan dauden fitxategiak idatz eta ezaba litzake. Ahultasun horretarako CVE-2019-11601 identifikatzailea erabili da.
- *Backup/Restore* funtzioak duen Server-Side Request Forgery (SSRF) erako ahultasun bat baliatuz, erasotzaile batek URL arbitrarioetarako GET eskaerak faltsutu litzake edo zerbitzari lokaleko zip fitxategiak irakurri. Ahultasun horretarako CVE-2019-11897 identifikatzailea erabili da.
- *Backup/Restore* funtzioaren urruneko sarbideetako pilaren aztarnaren filtrazioa baliatuz, urruneko erasotzaile batek sistemaren egiturari buruzko informazioa eskura lezake. Ahultasun horretarako CVE-2019-11602 identifikatzailea erabili da.
- HTTP bide jauziaren ahultasun bat baliatuz, erasotzaile batek web zerbitzariko errotik kanpoko fitxategiak irakur litzake. Ahultasun horretarako CVE-2019-11603 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Modu ezegokian babestutako kredentzialak Zebra-ren inprimagailu industrialetan

Argitalpen data: 2019/08/21

Garrantzia: Ertaina

Kaltetutako baliabideak:

- Zebra-ren inprimagailu industrial guztiak.

Azalpena:

Tri Quach ikertzaileak modu ezegokian babestutako kredentzialen erako ahultasun baten berri eman du, Zebraren inprimagailu industrialei eragiten diena. Hori baliatuz, urruneko erasotzaile batek bereziki diseinatutako paketeak bidal litzake inprimagailuaren ataka zehatz batera, aurrealdeko kontrol panelaren pasahitza eskuratzearren.

Konponbidea:

Link-OS v6.0 eguneraketa aplikatzea.

Xehetasuna:

Kode bitartez inprimagailuaren aurrealdeko panelera sartzeko aukera ezartzean, modu lehenetsian desgaituta datorrena, erasotzaile batek sarbide kodea eskura lezake bereziki diseinatutako paketeak bidaliz inprimagailuaren ataka batetara, sare beraren bitartez, eta horrela aurrealdeko paneleko funtzionaltasun guztietara sarbidea lortzeko erabil lezake.

Etiketak: Eguneraketa, Ahultasuna

Bufferraren gainezkatzea WECONen LeviStudioU-n

Argitalpen data: 2019/08/22

Garrantzia: Handia

Kaltetutako baliabideak:

- LeviStudioU.

Azalpena:

Zero Day Initiative-ko Mat Powell ikertzaileak bufferraren gainezkatze erako ahultasun baten berri eman du, WECONen LeviStudioU-ri eragiten diona. Hori baliatuz, urruneko erasotzaile batek kodea exekuta lezake administratzaile pribilegioekin.

Konponbidea:

Zerbitzuarekiko interakzioa konfiantzako makinei soilik baimentzea aholkatzen da.

Xehetasuna:

ShortMessage SMtext elementua aztertzean, prozesuak ez du zuzen balioztatzen erabiltzaileak emandako datuen luzera, luzera finkoko bufferrean kopiatu aurretik. Erasotzaile batek ahultasun hori balia lezake kodea exekutatzeko administratzaile pribilegioekin.

Etiketak: 0day, Ahultasuna

Bufferraren gainezkatzea Delta Controls-en enteliBUS Controllers-en

Argitalpen data: 2019/08/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- enteliBUS Manager, firmwarearen 3.40 R5 build 571848 bertsioa eta lehenagokoak;
- enteliBUS Manager Touch (eBMGR-TCH), firmwarearen 3.40 R5 build 571848 bertsioa eta lehenagokoak;
- enteliBUS Controller (eBCON), firmwarearen 3.40 R5 build 571848 bertsioa eta lehenagokoak.

Azalpena:

McAfee Advanced Threat Research-eko Douglas McKee eta Mark Bereza ikertzaileek Delta Controls-en enteliBUS Controllers ekipamenduari eragiten dion bufferraren gainezkatze erako ahultasun baten berri eman dute. Sare berean dagoen erasotzaile batek gailurako sarbide osoa lor lezake eta kodea exekutatu administratzaile pribilegioekin.

Konponbidea:

Delta Controls-ek enteliBUS 3.40 R6 build 612850 eguneraketa argitaratu du.Firmware berri hau partner erregistratuek soilik eskura dezakete. Eguneraketa lortzeko Delta Controls-ekin edo banatzaile batekin harremanetan jartzea gomendatzen da.

Xehetasuna:

Bufferraren gainezkatze erako ahultasunaren arrazoia sarreraren baliozkotze falta da. Erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2019-9569 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Autentifikazioari ihesa Datalogic-en AV7000 Linear Barcode Scanner-en

Argitalpen data: 2019/08/28

Garrantzia: Handia

Kaltetutako baliabideak:

4.6.0.0 bertsioaren aurreko AV7000ren bertsio guztiak

Azalpena:

Amazon-en Customer Fulfillment Technology Security (CFS) taldeko Tri Quach eta Blake Johnson ikertzaileek Datalogic-en AV7000-k duen autentifikazioari ihes erako ahultasun baten berri eman dute.

Konponbidea:

Datalogic-ek jakinarazi du ahultasun hori konpontzen duen firmwarearen bertsio berri bat argitaratu duela. Kaltetutako erabiltzaileak Datalogic-ekin jarri behar dira harremanetan bertsio hori eskuratzeko.

Xehetasuna:

Kanal edo bide alternatibo baten bidez egiten den autentifikazioaren ihes erako ahultasuna baliatuz, erasotzaile batek urruneko kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2019-13526 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Funtzio zaharkituen erabilpena Philips-en HDI 4000 Ultrasound Systems-en

Argitalpen data: 2019/08/30

Garrantzia: Txikia

Kaltetutako baliabideak:

Philips HDI 4000 Ultrasound Systems, sistema eragile zaharretan eta zerbitzurik gabekoetan, adibidez Windows 2000, exekutatzen diren bertsio guztiak.

Azalpena:

Check Point-ek funtzio zaharkituen erabilpen erako ahultasun baten berri eman du, Philips-en HDI 4000 Ultrasound Systems ekipamenduari eragiten diona. Ultrasoinuen irudiak ezagutzera ematea eta horien integritatea arriskuan jartzea ahalbidetu dezake.

Konponbidea:

Produktu honen zerbitzuaren epealdia 2013ko abenduaren 31n amaitu zen, eta hortaz ez da espero behar zerbitzurik edo eguneraketarik Philips-en aldetik. Erabiltzaileek kontrolak ezarri beharko dituzte sarerako sarbidea mugatzeko, eta produktua berriago batekin ordezkatzea aztertu beharko lukete, zerbitzua duen sistema eragile batekin.

Xehetasuna:

HDI 4000 Ultrasound System sistema eragile zahar eta zerbitzurik ez duen batean integratuta dago. Hortaz, sistema eragile horren edozein ahultasunek produktuari eragin liezaioke. Ahultasun horretarako CVE-2019-10988 identifikatzailea erabili da.

Etiketak: Ahultasuna

Lehenetsitako baimen okerrak Change Healthcare-ren ekipoetan

Argitalpen data: 2019/08/30

Garrantzia: Handia

Kaltetutako baliabideak:

- Horizon Cardiology, 12.x eta lehenagoko bertsioak;
- McKesson Cardiology, 14.x eta 13.x adarretako bertsioak;
- Change Healthcare Cardiology, 14.1.x adarreko bertsioak.

Azalpena:

Asante Information Security taldeko Alfonso Powers eta Bradley Shubin ikertzaileek kritikotasun altuko ahultasun baten berri eman dute, Change Healthcare-ren ekipamenduari eragiten diona. Autentifikatutako erasotzaile lokal batek kode arbitrarioa exekuta lezake.

Konponbidea:

Change Healthcare-k kaltetutako erabiltzaileei gomendatzen die beren zerbitzu departamentuarekin harremanetan jartzea lehenbailehen, partxearen instalazioa egitearren.

Xehetasuna:

Ahultasunaren arrazoia sistemaren lehenetsitako instalazioan fitxategi batzuen baimen ez-seguruak dira. Sistemara sarbide lokala lukeen erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2018-18630 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna