2018ko Urriaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Hainbat ahultasun Entes-en EMG 12-n

Argitalpen data: 2018/10/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Gateways EMG12 Ethernet Modbus-en firmwarea, 2.57 eta lehenagoko bertsioak

Azalpena:

Biznet Bilisim-eko Can Demirel ikertzaileak autentifikazio desegoki eta informazioaren agerpen erako hainbat ahultasunen berri eman du. Horiek baliatuz erasotzaile batek baimenik gabeko sarbidea lor lezake edo gailuen konfigurazioak alda litzake.

Konponbidea:

- Entes EMGk erabiltzaileei aholkatzen die eskuragarri dagoen firmwarearen azken bertsiora eguneratzea.

Xehetasuna:

- Aplikazioak erabiltzen duen web interfazean posible da erasotzaile batek autentifikazioa saihestea bereziki diseinatutako URL baten bidez. Honek kodea urrunetik exekutatzea ahalbidetu lezake. Ahultasun horretarako CVE-2018-14826 identifikatzailea erabili da.
- Web interfazeak duen kontsulten kate erako ahultasunaren bidez informazioaren agerpena gertatzen dela ikusi da. Hori baliatuz erasotzaile batek erabiltzaile legitimo bat ordezka lezake eta kode arbitrarioa exekutatu. Ahultasun horretarako CVE-2018-14822 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Bufferraren gainezkatzea Delta Electronics-en ISPSoft-en

Argitalpen data: 2018/10/03

Garrantzia: Ertaina

Kaltetutako baliabideak:

- ISPSoft, 3.0.5 bertsioa eta lehenagokoak

Azalpena:

Zero Day Initiativeko Ariele Caltabianok (kimiya) Delta Electronics-en ISPSoft produktuari eragiten dion bufferraren gainezkatze erako ahultasun baten berri eman du. Hori baliatuz erasotzaile batek kodea exekuta lezake aplikazioaren testuinguruan.

Konponbidea:

- Delta Electronics-ek erabiltzaile kaltetuei gomendatzen die ISPSoft 3.0.6 edo goragoko bertsiora eguneratzea.

Xehetasuna:

- Erasotzaile batek bereziki aldatutako fitxategi bat erabil lezake aplikazioak fitxategia irekitzean pilaren objektu bati ezarritako mugatik harago irakur dezan. Horrek kodea exekutatzea ahalbidetu lezake aplikazioaren testuinguruan. Ahultasun horretarako CVE-2018-14800 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Wecon-en PIStudio-n

Argitalpen data: 2018/10/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- PIStudio

Azalpena:

Natnael Samson ikertzaile independenteak eta Trend Microren Zero Day Initiative-ko (ZDI) Mat Powell-ek bufferraren gainezkatzea, mugez kanpoko irakurketa eta idazketa eta informazioaren zabalkunde erako hainbat ahultasun aurkitu dituzte Wecon-en PIStudio produktuan. Erasotzaile batek kode arbitrarioa exekuta lezake eta informazio sentikorra zabaldu.

Konponbidea:

Ahultasunen berri eman da partxerik oraindik egon gabe, ZDIk duen 120 eguneko zabalkunde politika dela eta.

ZDIk prebentzio neurri modura proposatzen du kaltetutako produktuek konfiantzako fitxategiekin soilik interaktuatzea.

Xehetasuna:

- Bufferrak gainezka egitea: hsc fitxategien maneiatzaileak ez du ondo balioztatzen erabiltzaileak emandako datuen luzera, luzera finkoko buffer batean kopiatu aurretik. Erasotzaile batek kode arbitrarioa exekutatzea lor lezake pribilegio altuekin.
- Mugez kanpoko irakurketa: DAT fitxategien barneko irudien kudeaketa ez da zuzen egiten eta erabiltzailearen datuak ez dira zuzen balioztatzen. Gerta liteke gainera objektuaren amaieraren ondoreneko posizioak ere irakurtzea. Erasotzaile batek ahultasun hori balia lezake beste batzuekin batera, kodea urrunetik exekutatu ahal izatearren.
- Mugez kanpoko idazketa: hsc fitxategien maneiatzaileak ez du ondo balioztatzen erabiltzaileak emandako datuen luzera, eta horrek eragin lezake objektuarentzat erreserbatutako mugen ondoreneko posizioetan idaztea. Horrela, erasotzaile batek kode arbitrarioa exekutatzea lor lezake.
- Informazioa zabaltzea: proiektuaren fitxategien prozesamenduak ez dauka kanpoko XML entitateetarako (XXE) erreferentzien murrizpenik. Ondorioz, erasotzaile batek bereziki manipulatutako dokumentu bat erabil lezake eta informazio zehatzera baimenik gabeko sarbidea lortu.

Etiketak: 0day, Ahultasuna

Schneider Electric etxearen Modicon M221 tresnan ez da datuen egiazkotasuna behar bezala egiaztatu

Argitaratze-data: 2018/10/04

Garrantzia: Handia

Kaltetutako baliabideak:

- Modicon M221, bertsio guztiak.

Azalpena:

CRITIFENCE-ko Eran Goldstein ikertzaileak, Schneider Electric-ekin batera, antzeman du Schneider Electric etxearen Modicon M221 tresnan ez dela behar beste kontrolatu datuen egiazkotasuna. Horren ondorioz, erasotzaile batek IPv4 konfigurazioa aldatu lezake, gailura urrutitik sartzean.

Konponbidea:

Fabrikatzaileak honako neurriak hartzea gomendatu du:

- 502 porturako kanpoko edo barruko sarbidea blokeatzen duen suebaki bat konfiguratzea.
- Modicon M221 aplikazioaren barruan, erabiltzaileak erabiltzen ez diren protokolo guztiak desgaitu behar ditu, bereziki programazio protokoloa, SoMachine Basic-en laguntza lineako ?Configuración de la red Ethernet? atalean azaltzen den moduan. Horrela, PLC M221 tresnaren urrutiko programazioa prebenituko da.

Xehetasuna:

- Erasotzaile batek aldaketa bat eragin lezake IPv4 tresnaren konfigurazioan (IP helbidea, maskara eta gateway), datuak behar den moduan ez egiaztatzearen ondorioz, gailura urrutitik sartzean. Ahultasun horretarako, CVE-2018-7798 identifikatzailea erreserbatu da.

Etiketak: Schneider Electric, Ahultasuna

Moxaren EDR-810 Series router industrialaren komandoen injekzioa

Argitaratze-data: 2018/10/08

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- EDR-810 Series, 4.2 firmware bertsioa edo aurrekoa duena.

Azalpena:

Moxak komando injekzio motako ahultasun bat antzeman du EDR-810 routerren web zerbitzarian. Ahultasun hori baliatuta, urrutiko erasotzaile batek kaltetutako gailuaren sistema eragilean komandoak exekutatu litzake, supererabiltzaile baimenekin.

Konponbidea:

Moxak ahultasun hori konpondu du, kaltetutako gailurako firmware bertsio berri bat argitaratuz.

Firmwarearen bertsio berria lotura honetan deskargatu daiteke: https://www.moxa.com/support/download.aspx?type=support&id=15851

Xehetasuna:

Urrutiko erasotzaile batek Moxaren web zerbitzariko komandoen injekzio motako ahultasun bat baliatu lezake, sistema eragilean komandoak exekutatzeko supererabiltzaile pribilegioekin, /xml/net_WebCADELETEGetValue URLean dagoen *caname* parametroaren bidez. Ahultasun horretarako, CVE-2018-16282 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Nabigatzailea, Ahultasuna

Informazioa zabaltzea Change Healthcare-ren PeerVue Web Server produktuan

Argitaratze-data: 2018/10/08

Garrantzia: Txikia

Kaltetutako baliabideak:

- PeerVue Web Server bertsio guztiak, 7.6.2-ra arte.

Azalpena:

Zingbox-eko Dan Regalado ikertzaileak informazioaren zabalkunde motako ahultasun bat antzeman du Change Healthcare etxearen PeerVue Web Server produktuan. Erasotzaile batek PeerVue Web Server produktuari buruzko informazio teknikoa lortu dezake eta ondoren beste eraso baterako erabili.

Konponbidea:

Change Healthcare etxeak ahultasun hori konpontzeko partxe bat atera du. Erabiltzaileek Change Healthcareko asistentzia taldearekin harremanetan jarri behar dute, partxe horren inguruko informazioa lortzeko.

Xehetasuna:

Erasotzaile batek zerbitzariarekiko HTTP komunikazioen erroreen kudeaketaren akats bat baliatu lezake, informazio tekniko gehiago lortzeko. Ahultasun horretarako, CVE-2018-10624 identifikatzailea esleitu da.

Etiketak: Ahultasuna

Informazioa zabaltzea Carestream etxearen Vue RIS produktuan

Argitaratze-data: 2018/10/08

Garrantzia: Txikia

Kaltetutako baliabideak:

- RIS Client Builds, 11.2 bertsioa eta aurrekoak, IIS 7.5 daukan Windows 8.1 sistema batean funtzionatzen.

Azalpena:

Zingbox-eko Dan Regalado ikertzaileak informazio zabalkunde motako ahultasun bat antzeman du Carestream-en Vue RIS produktuan. Erasotzaile batek informazio filtratua lortu dezake eta gerora eraso bat egiteko erabili.

Konponbidea:

Carestream-ek ahultasun hori konpondu du softwarearen egungo bertsioan eta honako konponbideak eman ditu kaltetuta egon daitezkeen bertsio zaharretarako:

- RIS 11.2 bertsiorako, Windows 8.1 eta IIS 7.2-ekin exekutatzen dena:
  - ?Show debug messages? Desgaitzea.
  - Bezero/zerbitzari komunikazioetarako SSL gaitzea.

Xehetasuna:

Carestream zerbitzari batekin konektatu eta Oracle TNS listener zerbitzua eskuragarri ez egotekotan, HTTP 500 errore bat emango da eta informazio teknikoa filtratuko da. Erasotzaile batek informazio tekniko hori erabil lezake eraso landuago bat egiteko. CVE-2018-17891 identifikatzailea esleitu zaio.

Etiketak: Ahultasuna

Hainbat ahultasun Auto-Maskin produktu batzuetan

Argitaratze-data: 2018/10/08

Garrantzia: Handia

Kaltetutako baliabideak:

- Urrutiko Auto-Maskin RP 210E panelak
- DCU 210E kontrol unitateak
- Mugikorretarako Marine Pro Observer monitorizazio aplikazioa.

Azalpena:

Brian Satira eta Brian Olson ikertzaileek mota honetako hainbat ahultasunen berri eman dute: pasahitz barneratua, jakinarazpenen balioztatze okerra eta datu sentikorrak testu lau gisa transmititzea. Ahultasun horiek urrunetik baliatu daitezke eta erasotzaileren batek sarean konektatuta dauden unitate eta motorretarako sarbidea izan dezake, informazio sentikorra berez transmititzeko.

Konponbidea:

Prebentzio neurri moduan, kaltetutako gailuak isolatzea gomendatu da; horrela, aseguratutako sare pribatuetatik soilik izango dira irisgarriak.

Xehetasuna:

- **Pasahitz barneratuak:** DCU 210E gailuaren firmwareak kredentzial barneratuak dituen dokumentatu gabeko dropbear SSH zerbitzari bat dauka. Gainera, pasahitza erraz crackeatu daiteke. Ahultasun horretarako, CVE?2018-5399 identifikatzailea esleitu da.
- **Jakinarazpenen balioztatze okerra:** Auto-Maskin produktuek dokumentatu gabeko protokolo pertsonalizatu bat erabiltzen dute beste gailu batzuekin Modbus jakinarazpenak konfiguratzeko, balioztatu beharrik gabe. Ahultasun horretarako, CVE?2018-5400 identifikatzailea esleitu da.
- **Informazio sentikorra testu lau gisa transmititzea:** Kaltetutako gailuek prozesuaren informazio sentikorra transmititzen dute, zifratu gabeko Modbus jakinarazpenen bidez. Ahultasun horretarako, CVE?2018-5401 identifikatzailea esleitu da.
- **Informazio sentikorra testu lau gisa transmititzea:** Barneratutako web zerbitzariak testu lau motako jakinarazpenak erabiltzen ditu, administrariaren PIN kodea transmititzeko. Ahultasun horretarako, CVE?2018-5402 identifikatzailea esleitu da.

Etiketak: Jakinarazpenak, Nabigatzailea, Ahultasuna

General Electric-en iFix HMI produktuetarako Gigasoft-en ActiveX osagaiaren ahultasuna

Argitaratze-data: 2018/10/10

Garrantzia: Ertaina

Kaltetutako baliabideak:

- iFIX tresnaren 2.0tik 5.0era bitarteko bertsioak.
- 5.1, 5.5 eta 5.8 iFIX bertsioak

Azalpena:

360 aegis-eko LiMingzheng ikertzaileak ActiveX tresnaren kontrol ez seguruaren ahultasun honen berri eman du, *scripting*-erako seguru gisa markatua. Ahultasun hori baliatuta, erasotzaile batek bufferrak gainezka egitea eragin dezake.

Konponbidea:

Fabrikatzaileak 5.9 iFIX bertsioa kaleratu zuen 2017ko ekainean, osagaiaren Gigasoft 8.0 bertsioan arazo hori konpontzeko.

General Electric etxeak erabiltzaileei gomendatu die ActiveX tresna konfiantzazko iturriekin soilik erabiltzeko.

Xehetasuna:

- **ActiveX objektuaren kontrol ez segurua, *scripting*-erako seguru gisa markatua:** Ahultasun horren hainbat instantzia identifikatu dira, Gigasoft-ek General Electric iFIX tresnari emandako hirugarrenen ActiveX objektuan. Gigasoft grafiko-paketea iFIX produktutik kanpo modu independentean erabiltzeak soilik jar ditzake erabiltzaileak ahultasun honen mende. Internet Explorerri eragiten dion metodoa ez dago IFIX produktuan, eta ez dakigu kaltetutako iFIX produktuaren funtzionalitate nagusia den. Ahultasun horretarako, CVE?2018-17925 identifikatzailea esleitu da.

Etiketak: Ahultasuna

DLL Hijacking motako ahultasuna Fuji Electric etxearen Energy Savings Estimator sisteman

Argitaratze-data: 2018/10/10

Garrantzia: Handia

Kaltetutako baliabideak:

- Fuji Electric Energy Savings Estimator, 1.0.2.0 bertsioa eta aurrekoak.

Azalpena:

Karn Ganeshen ikertzaileak DLL Hijacking motako ahultasunaren berri eman dio NCCIC erakundeari. Ahultasun hori baliatuta, erasotzaile batek DLL maltzur bat kargatu lezake eta kode bat exekutatu, sistemaren funtzionamenduari eraginez.

Konponbidea:

Fuji Electric etxeak produktua 1.0.2.1 bertsiora eguneratzea gomendatu du.

Xehetasuna:

- **DLL Hijacking:** Ahultasun hori arrakastaz baliatuta, erasotzaile bat sisteman sar liteke, DLL maltzurra exekutatzen duen aplikazioaren pribilegio berdinekin. Ahultasun horretarako, CVE-2018-14812 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna

Hainbat ahultasun Siemensen produktuetan

Argitaratze-data: 2018/10/10

Garrantzia: Handia

Kaltetutako baliabideak:

- SCALANCE W1750D, 8.3.0.1 bertsioaren aurreko guztiak.
- ROX II, 2.12.1 bertsioaren aurreko guztiak.
- CPU SIMANTIC S7-1200 familia, 4.2.3 bertsioaren aurreko guztietan.
- SIMATIC S7-1500 (F barne), 2.5 bertsioaren aurreko guztiak, 2.0 barne.
- SIMATIC S7-1500 software kontrolagailua, 2.5 bertsioaren aurreko guztiak, 2.0. barne.
- SIMATIC ET-200SP Open Controller, 2.0 bertsioaren aurreko guztiak, 2.0 barne.
- RUGGEDCOM APE, bertsio guztiak.
- RUGGEDCOM RX1400 VPE, bertsio guztiak.
- SIMATIC Field PG M4, 18.01.09 bertsioaren aurreko BIOS bertsio guztiak.
- SIMATIC Field PG M5, 22.01.06 bertsioaren aurreko BIOS bertsio guztiak.
- SIMATIC IPC227E, bertsio guztiak.
- SIMATIC IPC277E, bertsio guztiak.
- SIMATIC IPC3000 SMART V2, bertsio guztiak.
- SIMATIC IPC327E, bertsio guztiak.
- SIMATIC IPC347E, bertsio guztiak.
- SIMATIC IPC377E, bertsio guztiak.
- SIMATIC IPC427C, bertsio guztiak.
- SIMATIC IPC427D, V17.0X.14 bertsioaren aurreko BIOS bertsio guztiak.
- SIMATIC IPC427D, V21.01.09 bertsioaren aurreko BIOS bertsio guztiak.
- SIMATIC IPC477C, bertsio guztiak.
- SIMATIC IPC547E, bertsio guztiak.
- SIMATIC IPC547G, bertsio guztiak.
- SIMATIC IPC627C, bertsio guztiak.
- SIMATIC IPC627D, bertsio guztiak.
- SIMATIC IPC647C, bertsio guztiak.
- SIMOTION P320-4S, bertsio guztiak.

Azalpena:

P3 Communications GmbH-eko Lisa Fournet eta Marl Joos eta Poloniako Ikerketa Nuklearraren Zentro Nazionaleko Marcin Dudek, Jacek Gajewski, Kinga Staszkiewicz, Jakub Suchorab eta Joanna Walkiewicz ikertzaileek, Siemensekin elkarlanean, mota hauetako hainbat ahultasun antzeman dituzte: arazo kriptografikoak, pribilegioen kudeaketa okerra, CSRF, sarbideen balioztatze okerra eta informazio sentikorra zabaltzea. Ahultasun horiek baliatuta, erasotzaile batek gailu desberdinetarako urrutiko sarbidea edukiko luke eta komandoak exekutatu ahal izango lituzke; informazio sentikorra lortu edota zerbitzu ukapenak sortu.

Konponbidea:

- **Arazo kriptografikoak:** Siemensek 8.3.0.1 firmwarearen eguneraketa bat eskaini du eta erabiltzaileei gomendatu die bertsio berrira eguneratzeko. Lotura honetan deskargatu daiteke: https://support.industry.siemens.com/cs/us/en/view/109760581. Arriskua murrizteko, Siemensek administrariei aholkatu die kaltetutako gailuetan interfazerako sarbidea mugatzeko.
- **Pribilegioak behar ez den moduan kudeatzea:** Siemensek erabiltzaileei gomendatu die 2.12.1 bertsio berrira eguneratzeko. Lotura honetan deskargatu daiteke: https://support.industry.siemens.com/cs/us/en/view/109760683. Arriskua murrizteko, Siemensek administrariei gomendatu die sarerako sarbidea mugatzeko, erasotzaileak 22/TCP portura sartu ezin izateko.
- **CSRF**: Siemensek 4.2.3 firmwarearen eguneraketa bat eskaini du eta erabiltzaileei gomendatu die ahalik eta arinen eguneratzeko. Firmwarearen bertsio berria lotura honetan deskargatu daiteke: https://support.industry.siemens.com/cs/us/en/view/109741461. Arriskua murrizteko, Siemensek erabiltzaileei gomendatu die kaltetutako gailuetan erregistratuta dauden bitartean web nabigatzailearekin ez ibiltzeko.
- **Sarbidearen balioztatze okerra:** Siemensek eguneraketak eskaini ditu kaltetutako sistemetan ahultasun hori konpontzeko. Lotura hauetan deskarga ditzakezu ahultasuna konpontzeko eguneraketak:
  - SIMATIC S7-1500 software kontrolatzailea: https://support.industry.siemens.com/cs/us/en/view/109478528
  - SIMANTIC S7-1500: https://support.industry.siemens.com/cs/us/en/ps/13717/dl

Prebentzio neurri moduan, Siemensek hainbat gomendio eman ditu:

- Kaltetutako gailuen sarerako sarbidea mugatzea.
- ?cell-protection? eta ?defense-in-depth? Kontzeptua aplikatzea.

Xehetasuna:

- **Arazo kriptografikoak:** Kaltetutako gailuak dauden sarerako sarbidea duen erasotzaile batek TLS saiorako gako bat lor dezake. Erasotzaileak erabiltzaile eta gailuaren arteko TLS trafikoa hartuko balu, trafiko hori deszifratu ahal izango luke. Ahultasun horretarako, CVE-2017-13099 identifikatzailea esleitu da.
- **Pribilegioak behar ez den moduan kudeatzea:**
  - 22/TCP porturako sare bidezko sarbidea eta kaltetutako gailurako pribilegio gutxiko erabiltzaile baten kredentzialak izatekotan, erasotzaile batek pribilegioak handitu litzake eta supererabiltzailearen pribilegioak lortu. Ahultasun horretarako, CVE-2018-13801 identifikatzailea esleitu da.
  - SSH interfazearen bidez 22/TCP portuan pribilegio handiko erabiltzaile baten kontura sartzea lortzen duen erasotzaile batek mugaketak saihestu eta komandoak arbitrarioki exekutatu litzake. Ahultasun horretarako, CVE-2018-13802 identifikatzailea esleitu da.

- **CSRF:** Web interfazeak aukera emango lioke erasotzaile bati CSRF eraso teknika erabiltzeko eta kaltetutako gailuan erregistratutako erabiltzaileak engainatzeko, hainbat lotura maltzur erabiliz. Erasotzaile batek egiaztatutako erabiltzaile baten interakzioa beharko luke. Horrela, ahultasun hori baliatuta, erasotzaileek ekintza maltzur bat burutu ahal izango lituzke web interfazearen bidez. Ahultasun horretarako, CVE-2018-13800 identifikatzailea esleitu da.
- **Sarrerako balioztatze okerra:** Erasotzaile batek zerbitzu ukapen bat sortu lezake sarean, PLCra bereziki osatutako pakete kopuru handi bat bidaliz. Kaltetutako sistemetan sareko sarbidea daukan erasotzaile batek ahultasun hori baliatu lezake. Ahultasun hori baliatzeko ez da pribilegiorik edo erabiltzaileen interakziorik behar. Erasotzaile batek ahultasun hori erabili lezake sareko eskuragarritasuna konprometitzeko. Ahultasun horretarako, CVE-2018-13805 identifikatzailea esleitu da.
- **Informazio sentikorra zabaltzea** (hainbat ahultasun): Intelen software luzapenak eta espekulazioa erabiltzen dituzten mikroprozesagailuen sistemen bidez, L1 datu cachean dagoen informazioa baimenik gabe zabaldu ahal izango luke tokiko erabiltzailearen sarbidea daukan erasotzaile batek. Ahultasun hauetarako honako identifikatzaileak esleitu dira: CVE-2018-3615, CVE-2018-3620 eta CVE-2018-3646.

Etiketak: Eguneratzea, Siemens, Ahultasuna

Hainbat ahultasun Nuuoren produktu batzuetan

Argitaratze-data: 2018/10/15

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- NVRmini2 eta NVRsolo 3.8.0 bertsioa eta aurrekoak
- CMS 3.1 bertsioa eta aurrekoak.

Azalpena:

Pedro Ribeiro, Ariele Caltabiano (kimiya) 9SG Security Team-eko ikertzaileek eta Trend Microko Mat Powell ikertzaileak mota hauetako hainbat ahultasun antzeman dituzte: Buferrak gainezka egitea, sobera dagoen garbiketa kodea, aleatoriotasun nahikorik gabeko balioen erabilera, funtzio zaharkituen erabilera, baimenak oker ematea eta kredentzial barneratuak. Erasotzaile batek kodearen urrutiko exekuzioa egitea lortu lezake eta erabiltzailearen kontuak aldatu.

Konponbidea:

- NVRmini2 eta NVRsolo-rako, 3.9.1 firmware bertsiora eguneratu.
- CMS-rako, 3.3 firmware bertsiora eguneratu.

Xehetasuna:

- Bufferraren gainezkatzea baliatuz, egiaztatu gabeko erasotzaile batek kodea urrutitik exekutatu lezake. Ahultasun horretarako, CVE-2018-1149 identifikatzailea erreserbatu da.
- Urrutiko erasotzaile batek sisteman dauden fitxategiak baliatu litzake sartzea lortu eta erabiltzaileen datu sentikorrak aldatzeko. Ahultasun horretarako, CVE-2018-1150 identifikatzailea erreserbatu da.
- Erasotzaile batek aktibo dagoen saioaren ID lortu lezake, saioen identifikazio-mekanismoak sortua, eta kodea urrutitik exekutatu. Ahultasun horretarako, CVE-2018-17888 identifikatzailea erreserbatu da.
- Aplikazioak erabilitako funtzio zaharkitu eta ez seguruen bidez, urrutiko kodea exekutatu lezake. Ahultasun horretarako, CVE-2018-17890 identifikatzailea erreserbatu da.
- Erabiltzaileen kontuen kontrol metodoak ez ditu modu egokian hasten erabiltzaileen kontuen segurtasun ezaugarriak. Horren ondorioz, erasotzaile batek kodearen urrutiko exekuzioa burutu lezake. Ahultasun horretarako, CVE-2018-17892 identifikatzailea erreserbatu da.
- Aplikazioak berez sortutako kontuek kredentzial barneratuak dituzte, beraz, erasotzaile batek sarbide pribilegiatua lortu lezake. Ahultasun horretarako, CVE-2018-17894 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Ahultasuna

Hainbat ahultasun Delta Electronics-en TPEditor produktuan

Argitaratze-data: 2018/10/15

Garrantzia: Ertaina

Kaltetutako baliabideak:

- Delta Industrial Automation TPEditor, 1.90 bertsioa eta aurrekoak.

Azalpena:

9SG Security Team-eko Ariele Caltabianok eta Mat Powellek, Zero Day Initiative ekimenarekin elkarlanean, Delta Electronics-en TPEditor tresnari eragiten dioten hainbat ahultasun antzeman dituzte, bufferraren gainezkatze eta mugetatik kanpoko idazketa motakoak. Erasotzaile batek kode arbitrarioa exekutatu lezake eta informazio sentikorra zabaldu.

Konponbidea:

Delta Electronics enpresak TPEditor tresnaren 1.91 bertsioa argitaratu du, ahultasun horiek konpontzeko.

Xehetasuna:

- Bereziki manipulatutako fitxategi baten bidez, erasotzaile batek erabiltzailearen sarrera-datuen balioztatze falta baliatu lezake proiektu-fitxategitik multzora kopiatu aurretik; horrela, kodea urrutitik exekutatzea lortu dezake. Ahultasun horretarako, CVE-2018-17929 identifikatzailea esleitu da.
- Erasotzaile batek kodea urrutitik exekutatu lezake, bereziki manipulatutako fitxategi bat erabiliz; erabiltzailearen sarrera-datuen balioztatze-falta baliatu lezake eta esleitutako mugetatik kanpo idatzi. Ahultasun horretarako, CVE-2018-17927 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna

Hainbat ahultasun LCDS -ren LAquis SCADA produktuan

Argitaratze-data: 2018/10/17

Garrantzia: Handia

Kaltetutako baliabideak:

- LAquis SCADA Smart Security Manager, 4.1.0.3870 bertsioa eta aurrekoak.

Azalpena:

Zero Day Initiative (Trend Micro) ekimeneko Mat Powell, 9SG Security Team-eko rgod, Source Incite-ko Esteban Ruiz, @garage4hackers-eko b0nd eta Ashraf Alharbi ikertzaileek, Zero Day Initiative ekimenarekin elkarlanean, hainbat ahultasunen berri eman dute, mota hauetakoak: bufferrak gainezka egitea, mugetatik kanpoko irakurketa eta idazketa, erakusle ez fidagarriaren erreferentzia eza eta direktorio mugatuen ibilbideen kontrol ez zuzena (Path traversal). Ahultasun horiek arrakastaz burututa, urrutiko erasotzaile batek kode arbitrarioa exekutatu lezake, xede-sisteman edukia idatzi edo sistema blokeatu.

Konponbidea:

LCDS enpresak erabiltzaileei proposatu die 4.1.0.4114 bertsiora eguneratzea.

Xehetasuna:

- Erakusle ez fidagarriaren erreferentzia ezaren ondorioz, kodea urrunetik exekutatu ahal izatea eragin daiteke. Ahultasun horretarako, CVE-2018-17893 identifikatzailea esleitu da.
- Mugetatik kanpoko irakurketaren ahultasun bat antzeman da. Horrela izanik, urrutiko erasotzaile batek kodea exekutatu lezake kaltetutako produktuetan. Ahultasun horretarako, CVE-2018-17895 identifikatzailea esleitu da.
- Bufferrak gainezka egitearen ondorioz, erasotzaile batek kodea exekutatu lezake urrutitik. Ahultasun horretarako, CVE-2018-17897 identifikatzailea esleitu da.
- Mugatutako direktorioetako ibilbideen kontrol ez zuzenaren ondorioz (path traversal), erasotzaile batek kodea urrutitik exekutatu lezake. Ahultasun horretarako, CVE-2018-17899 identifikatzailea esleitu da.
- Proiektu-artxiboak prozesatzen direnean, aplikazioak huts egiten du erabiltzailearen sarrera datuak balioztatzean, multzoko objektu batean idazketa eragiketak burutu baino lehen. Horren ondorioz, erasotzaile batek kodea exekutatu lezake, exekutatzen ari den egungo prozesuan. Ahultasun horretarako, CVE-2018-17901 identifikatzailea esleitu da.
- Bufferrak gainezka egiten duen hainbat ahultasun antzeman dira. Urrutiko erasotzaile batek kodea urrutitik exekutatu lezake. Ahultasun horretarako, CVE-2018-17911 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna

Hainbat ahultasun antzeman dira Omron etxearen CX-Supervisor produktuan

Argitaratze-data: 2018/10/18

Garrantzia: Handia

Kaltetutako baliabideak:

- CX-Supervisor, 3.4.1.0 bertsioa eta aurrekoak

Azalpena:

Tend Micro-ren Zero Day Initiative ekimeneko Mat Powell, 9SG Security Team-eko Ariele Caltabiano eta @garage4hackers-eko b0nd ikertzaileak Tend Micro-ren Zero Day Initiative ekimenarekin batera aritu dira lanean eta Omron erakundearen CX-Supervisor softwarearen hainbat ahultasunen berri eman dute, mota hauetakoak: eragiketen mugatze akastuna memoria bufferraren mugen barruan, mugetatik kanpoko irakurketa, liberazioaren osteko baliabide erabilera eta moten eraldaketa ez zuzena. Urrutiko erasotzaile batek kode arbitrarioa exekutatu lezake aplikazioaren testuinguruan, objektuak hondatu edo aplikazioa bortxatu array baten kanpoko balio bat irakurtzera.

Konponbidea:

Omrom-ek ahultasun horiek konpontzeko 3.4.2 bertsioa jarri du abian. Erabiltzaileek honako loturan deskargatu dezakete: https://www.myomron.com/index.php?action=kb&article=1709.

Xehetasuna:

- Eragiketen mugatze akastuna memoria bufferraren mugen barruan. Erasotzaile batek proiektu-artxiboetako byte espezifiko bat manipulatu lezake eta memoria hondatu, objektu espezifiko baten tratamenduan. Ahultasun horretarako, CVE-2018-17905 identifikatzailea esleitu da.
- Mugetatik kanpoko irakurketa. Erasotzaile batek proiektu-artxiboak manipulatu litzake eta aplikazioa bortxatu array-tik kanpoko balio bat irakurtzera. Ahultasun horretarako, CVE-2018-17907 identifikatzailea esleitu da.
- Liberazioaren osteko baliabide erabilera. Proiektu-artxiboak prozesatzean, aplikazioa ez da gai liberatutako memoriari erreferentzia egiten zaion egiaztatzeko; horrela izanik, erasotzaile batek kodea exekutatu lezake aplikazioaren testuinguruan. Ahultasun horretarako, CVE-2018-17909 identifikatzailea esleitu da.
- Moten eraldaketa akastuna. Erasotzaile batek kode-exekuzio bat lortu lezake aplikazioaren testuinguruan, proiektu-fitxategien irakurketaren eraldatze-akats bat baliatuz. Ahultasun horretarako, CVE-2018-17913 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna

Hainbat ahultasun Moxaren ThingsPro IIoT Gateway produktuan

Argitaratze-data: 2018/10/18

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- ThingsPro Gateway 2.1 bertsioa

Azalpena:

Kaspersky Lab enpresako Alexander Nochvay ikertzaileak Moxaren ThingsPro Gateway tresnari eragiten dioten mota honetako hainbat ahultasun antzeman ditu: erabiltzaileen enumerazioa, pribilegioen handitzea, sarbide kontrol desegokia, pasahitzen aldaketa ahula, informazio sentikorra testu soil gisa gordetzea, kodea urrutitik exekutatzea. Urrutiko erasotzaile batek informazio sentikorra lortu lezake, pribilegioak handitu, pasahitzak aldatu edo kode bat urrutitik exekutatu.

Konponbidea:

Moxak gailuaren 2.3 firmware bertsioa askatu du, ahultasun horiek konpontzeko.
Erabiltzailearen enumerazioaren motako ahultasunerako, Moxak pasahitz seguruagoak erabiltzeko gomendatu die erabiltzaileei, honako irizpideak jarraituz:

- 8 karaktere gutxienez.
- Zenbakiak ere erabiltzea.
- Maiuskulak eta minuskulak erabiltzea.
- Karaktere bereziak erabiltzea.

Xehetasuna:

- Erabiltzaileen enumerazioa. Erasotzaile batek indar basatia erabil lezake webguneko erabiltzaileen pasahitzak lortzeko.
- Pribilegioak handitzea. Urrutiko erasotzaile batek ahultasun hori erabil dezake pribilegio gehiago lortzeko.
- Sarbide kontrol desegokia. Urrutiko erasotzaile batek ahultasun hori erabil dezake pribilegio gehiago lortzeko.
- Funtzio ez seguruak erabiltzea. Pasahitzak aldatzeko sistemak ez du pasahitz zaharra eskatzen, beraz, erasotzaile batek aukera hori baliatu lezake pasahitzak erraz aldatzeko.
- Informazio sentikorra testu arrunt gisa gordetzea. Ahultasun horrek aukera emango lioke erasotzaile bati tokenaren baimenak asmatzeko.
- Pribilegioak handitzea. Erasotzaile batek administrari pribilegioak lortu ditzake eta komandoak exekutatu, tokenaren ezkutuko API delakora sartuz.
- Kodearen urrutiko exekuzioa. Erasotzaile batek testu kateen injekzioa egin lezake eta zerbitzariari komando osagarriak exekutarazi.

Etiketak: Eguneratzea, Ahultasuna

Pribilegioak handitzeko ahultasuna PEPPERL FUCHS konpainiaren CT50-Ex tresnan

Argitaratze-data: 2018/10/19

Garrantzia: Handia

Kaltetutako baliabideak:

- CT50-Ex

Azalpena:

PEPPERL FUCHS fabrikatzaileak ahultasun bat antzeman du bere produktuetako batean. Hori dela eta, erasotzaileren batek pribilegioak handitu litzake eta eragindako produktuen informazio sentikorra lortu.

Konponbidea:

Fabrikatzaileak ahultasun hori konpontzeko eguneraketa bat argitaratu du.

- CT50-EX
  - Android 6.0
    - CommonES 4.01.00.4134 edo osteko bertsioen arabera eguneratzea.
    - ECP 2.30.00.0167 edo osteko bertsioetara eguneratzea (kasuaren arabera).
  - Android 4.4
    - CommonES 3.17.3445 edo osteko bertsioen arabera eguneratzea.

Xehetasuna:

- **Pribilegioak handitzea:** Androiden sistema eragilearen bidez exekutatzen den zerbitzuak ez ditu behar den moduan balioztatzen sartzen diren konexio eskaerak, beraz, erasotzaile batek teklen pultsazioak, pasahitzak, identifikatzeko moduko informazio pertsonala, argazkiak, posta elektronikoak edo enpresarentzako kritikoak diren dokumentuak ikus litzake. Ahultasun horretarako, CVE-2018-14825 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna

Hainbat ahultasun Advantech-en WebAccess

sisteman

Argitaratze-data: 2018/10/24

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- WebAccess, 8.3.1 bertsioa eta aurrekoak.

Azalpena:

Trend Microren Zero Day Initiative ekimeneko Mat Powell ikertzaileak mota hauetako hainbat ahultasun antzeman ditu: bufferrak gainezka egitea, ibilbideen edo fitxategien izenen kanpoko kontrola, pribilegioen kudeaketa desegokia eta direktorio-jauzia, Advantech-en WebAccessari eragiten diona. Urrutiko erasotzaile batek kodearen exekuzioa lortu lezake, fitxategietara sartu administrarien pribilegiodun ekintzak burutzeko edo sistematik fitxategiak ezabatzeko.

Konponbidea:

Advantech-ek WebAccessen 8.3.3 bertsioa argitaratu du, ahultasun horiek zuzentzeko.

Xehetasuna:

- Bufferrak gainezka egitea. Urrutiko erasotzaile batek bufferraren gainezkatze horietakoaren bat baliatu lezake kode arbitrarioa exekutatzeko. Ahultasun horretarako, CVE-2018-14816 identifikatzailea esleitu da.
- Ibilbideen edo fitxategien izenen kanpoko kontrola. Erasotzaile batek ibilbideen edo fitxategien izenen kanpoko kontrola baliatu lezake *dll* osagai batean, prozesatzeko unean fitxategiak arbitrarioki ezabatzeko. Ahultasun horretarako, CVE-2018-14820 identifikatzailea esleitu da.
- Pribilegioen kudeaketa desegokia. Urruneko erasotzaile batek ahultasun hori baliatu lezake administrari pribilegioak hartu eta sistemaren gaineko ekintzak burutzeko. Ahultasun horretarako, CVE-2018-14828 identifikatzailea esleitu da.
- Direktorio-jauzia. Erasotzaile batek kode arbitrarioa exekutatu lezake, ahultasun hori baliatuz. Ahultasun horretarako, CVE-2018-14806 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna

Network Card-MS ahultasuna Eaton-en UPSerako

Argitaratze-data: 2018/10/25

Garrantzia: Handia

Kaltetutako baliabideak:

- UPSerako Network Card-MS, LA bertsioan eta aurrekoetan.

Azalpena:

Eatonek ustezko ahultasun bat identifikatu du Network Card-MS txarteletan. Txartel horiek Eaton UPS monitorizatu eta kudeatzeko erabiltzen dira, LA bertsioko firmware batekin edo aurrekoarekin.

Konponbidea:

Eaton-ek ahultasun hori konpondu du, bere produktuak LB firmwarearen bertsio berriarekin eguneratuz, fabrikatzailearen web orritik.

Xehetasuna:

Ez da argitaratu gailu horri eragiten dion ahultasuna.

Etiketak: Ahultasuna

Hainbat ahultasun Advantech-en WebAccess sisteman

Argitaratze-data: 2018/10/26

Garrantzia: Handia

Kaltetutako baliabideak:

- WebAccess, 8.3.2 bertsioa eta aurrekoak.

Azalpena:

Trend Microren Zero Day Initiative ekimeneko Mat Powell ikertzaileak sarbide kontrol desegokiaren eta bufferrak gainezka egitearen motako hainbat ahultasun identifikatu ditu. Advantech-en WebAccess konponbideari eragiten diote eta, urrutiko erasotzaile batek kode arbitrarioa exekutatzea lortu lezake.

Konponbidea:

Advantech-ek WebAccessen 8.3.3 bertsioa argitaratu du, ahultasun horiek konpontzeko.

Xehetasuna:

· Erasotzaile batek kode arbitrarioa exekutatu lezake, aplikazioa instalatzeko prozesuan zehar sarbide kontrola desgaituta dagoela aprobetxatuz. Ahultasun horretarako, CVE-2018-17908 identifikatzailea erreserbatu da.

· Erabiltzaileak emandako sarbide-datuen luzera modu desegokian balioztatuz gero, erasotzaile batek bufferrak gainezka egitea eragin dezake eta, horrela, kode arbitrarioa exekutatu. Ahultasun horretarako, CVE-2018-17910 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna

Cross-site scripting ahultasuna GEOVAPen Reliance 4 SCADA/HMI produktuan

Argitaratze-data: 2018/10/26

Garrantzia: Ertaina

Kaltetutako baliabideak:

- Reliance 4 SCADA/HMI, 4.7.3 bertsioa, 3 eguneraketa eta aurrekoak.

Azalpena:

Ismail Mert ikertzaile independenteak sarrera-datuen neutralizazio desegokia motako ahultasun baten berri eman du (cross-site scripting). Horrek aukera emango lioke urrutiko erasotzaile bati proxy http bat erabili eta javascript kode arbitrario bat injektatzeko, http eskaera batean.

Konponbidea:

GEOVAPek 4.8 bertsioa argitaratuko du, ahultasun hori konpontzeko.

Xehetasuna:

- Baimenik gabeko urrutiko erasotzaile batek kode arbitrario bat injektatu lezake. Ahultasun horretarako, CVE-2018-17904 identifikatzailea esleitu da.

Etiketak: Eguneratzea, SCADA, Ahultasuna

DLLren bahiketa, Schneider Electric-en Schneider Electric Software Update (SESU) delakoan

Argitaratze-data: 2018/10/29

Garrantzia: Handia

Kaltetutako baliabideak:

- Schneider Electric Software Update (SESU), 2.2.0. SESU bertsioaren aurreko guztiak, Schneider Electric-en honako softwareak instalatuak dira:
  - Acti 9 Smart Test
  - Altiva rATV320DtmLibrary
  - AltivarDTMLibrary
  - AltivarMachine340DTMLibrary
  - AltivarProcessATV6xxDTMLibrary
  - AltivarProcessATV9xxDTMLibrary
  - Blue
  - CompactNSX Firmware Update
  - Ecodial Advance Calculation
  - eConfigure
  - Ecoreach Software
  - EcoStruxure Modicon Builder
  - eXLhoist Configuration Software
  - Lexium 26 DTM Library
  - Lexium 28 DTM Library
  - Lexium 32 DTM Library
  - LV Motor Starter
  - PowerSCADA Expert
  - Schneider Electric Floating License Manager
  - Schneider Electric License Manager
  - Schneider Electric Motion Sizer
  - Schneider Electric SQL Gateway
  - SoMachine Basic
  - SoMachine Motion Software
  - SoMachine Motion Tools V4.3
  - SoMachine Software
  - SoMove
  - SoSafe Configurable
  - SoSafe Programmable V2.1
  - TeSysDTM
  - Unity Loader
  - Unity Pro
  - Vijeo Citect
  - Vijeo Designer
  - Vijeo Designer Opti 6.1
  - Vijeo XD
  - Web Gate Client Files

Azalpena:

Venustec enpresako ADLab-eko Haojun Hou ikertzaileak, Schneider Electric-ekin lankidetzan, DLL bahiketa motako ahultasun bat

antzeman du; horren ondorioz, erasotzaile batek kode arbitrarioa exekutatu lezake.

Konponbidea:

Schneider Electric etxeak softwarearen 2.2.0 bertsioa argitaratu du, ahultasuna konpontzeko.

Xehetasuna:

- DLL bahiketaren ahultasun baten ondorioz, urrutiko erasotzaile batek kode arbitrarioaren exekuzioa burutu lezake sisteman. Ahultasun horretarako CVE-2018-7799 identifikatzailea esleitu da.

Etiketak: Eguneraketa, Schneider Electric, Ahultasuna

Hainbat ahultasun ABBren M2M ETHERNET eta CMS-770 sistemetan

Argitaratze-data: 2018/10/30

Garrantzia: Handia

Kaltetutako baliabideak:

- M2M ETHERNET Network analyser, 2.22 firmware bertsioa eta aurrekoak, Ethernet firmware 1.01 bertsioa eta aurrekoak.
- CMS-770 Control Unit, 1.71 bertsioa eta aurrekoak.
- Busch-EnergyMonitor, 1.71 bertsioa eta aurrekoak.

Azalpena:

Maxim Rupp ikertzaile independenteak, ABB-rekin elkarlanean, egiaztatze okerreko hainbat ahultasun identifikatu ditu, ABBren M2M ETHERNET eta CMS-770 produktuei eragiten dietenak. Erasotzaile batek fitxategiak karga litzake, edo gailu baten konfigurazioa irakurri eta kontrola bereganatu.

Konponbidea:

ABBk kaltetutako produktuen eskuliburuak eguneratu ditu eta erabiltzaileei gomendatu die jarraibideei kasu egiteko. Oraingoz, ez dago kaltetutako gailuetarako eguneraketarik.

Xehetasuna:

- Egiaztatu gabeko erasotzaile batek eskuz kargatu dezake hizkuntza artxibo bat, adierazpen ez baliagarriekin.
- Erasotzaile batek gailuaren konfigurazio-artxiboak irakur litzake; horrela, produktuaren kontrola hartzeko aukera emango luketen kredentzialak lortuko lituzke.

Etiketak: Ahultasuna