2018ko Irailaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Bufferraren gainezkatzea Opto22ren PAC Control Basic eta PAC Control Professional-en

Argitalpen data: 2018/09/05

Garrantzia: Handia

Kaltetutako baliabideak:

- AC Control Basic, R10.0a eta lehenagoko bertsioak
- PAC Control Professional, R10.0a eta lehenagoko bertsioak

Azalpena:

Robert Hawes ikertzaile independenteak bufferraren gainezkatze erako ahultasuna aurkitu du Opto22ren PAC Control Basic eta PAC Control Professionalen. Erasotzaile batek kodea urrunetik exekutatzea lor lezake.

Konponbidea:

- Opto22k erabiltzaileei aholkatzen die sistemak bertsio berrienera eguneratzea (R10.0b)

Xehetasuna:

- Kaltetutako produktuek akatsa ematen dute OptoScript blokean 63 karaktere baino gehiagoko eta espaziorik gabeko literal bat duen kate bat editatzen saiatzean. Erasotzaile batek ahultasun hori balia lezake kode arbitrarioa exekutatzeko. Ahultasun horretarako CVE-2018-04154 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna

Hainbat SQL injekzio ERPNext-en ERPNext-en

Argitalpen data: 2018/09/06

Garrantzia: Ertaina

Kaltetutako baliabideak:

- ERPNext, v10.1.6 (master) bertsioa

Azalpena:

Security Advisory EMEARko Yuri K ikertzaileak eman du SQL injekzio erako ahultasun hauen berri. Erasotzaile batek, web nabigatzaile baten bitartez eta tresna berezien beharrik gabe, bereziki diseinatutako web eskariak bidal litzake SQL injekzio bat eragiteko eta datuak arriskuan jartzeko.

Konponbidea:

- Oraingoz ahultasun hauetarako ez da inolako konponbiderik eskaini

Xehetasuna:

- Elementu berezien neutralizazio desegokia:
  - Searchfield parametroa SQL injekzio erako eraso bat exekutatzeko balia liteke. Ahultasun horretarako CVE-2018-3882 identifikatzailea erreserbatu da.
  - Employee eta sort_order parametroak SQL injekzio erako eraso bat exekutatzeko balia litezke. Ahultasun horretarako CVE-2018-3883 identifikatzailea erreserbatu da.
  - Sort_by eta start parametroak SQL injekzio erako eraso bat exekutatzeko balia liteke. Ahultasun horretarako CVE-2018-

3884 identifikatzailea erreserbatu da.
    - Order_by parametroa SQL injekzio erako eraso bat exekutatzeko balia liteke. Ahultasun horretarako CVE-2018-3885 identifikatzailea erreserbatu da.

Etiketak: 0day, Nabigatzailea, Ahultasuna

Hainbat ahultasun Ice Qube-ren Thermal Management Center-en

Argitalpen data: 2018/09/07

Garrantzia: Handia

Kaltetutako baliabideak:

- Thermal Management Center, 4.13 baino lehenagoko bertsio guztiak.

Azalpena:

Maxim Rupp ikertzaile independenteak Thermal Management Center gailuari eragiten dioten bi ahultasunen berri eman du. Erabiltzaileen autentifikazio desegokiarekin eta kredentzialak gordetzerakoan daukan babes faltarekin zerikusia dute. Urruneko erasotzaile batek ahultasun horiek balia litzake gailuan gordetako informazio sentikorra eskuratzeko.

Konponbidea:

Fabrikatzaileak ahultasun guztiak konpontzen dituen eguneraketa bat garatu du (v4.13 edo goragokoa) eta bere bezeroei aholkatzen die ekipoak ahalik eta azkarren eguneratzeko.

Xehetasuna:

- Autentifikazio desegokia: Thermal Management Center gailuaren web aplikazioak ez ditu erabiltzaileak modu egokian kudeatzen autentifikazioaren fasean. Urruneko erasotzaile batek ahultasun hori balia lezake sistemara sartzeko eta informazio sentikorra eskuratzeko. Ahultasun horretarako CVE-2017-14026 identifikatzailea erreserbatu da.
- Babes falta kredentzialen biltegiratzean: gailuaren pasahitzak testu lauan gordeta daude autentifikaziorik gabe eskura daitekeen fitxategi batean. Urruneko erasotzaile batek ahultasun hori balia lezake informazio sentikorra eskuratzeko eta ondoren eraso landuagoak egiteko. Ahultasun horretarako CVE-2017-16714 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Pribatutasuna, Ahultasuna

Hainbat ahultasun Fuji Electric-en V-Server eta V-Server Lite-n

Argitalpen data: 2018/09/12

Garrantzia: Handia

Kaltetutako baliabideak:

- V-Server VPR, 4.0.3.0 bertsioa eta lehenagokoak
- V-Server Lite, 4.0.3.0 bertsioa eta lehenagokoak

Azalpena:

Source Inciteko Steven Seeley ikertzaileak eta Ariele Caltabiano ikertzaileak, Trend Microko Zero Day Initiativerekin lankidetzan, ahultasun hauen berri eman dute. Horiek baliatuz erasotzaile batek urrunetik kodea exekuta lezake, gailuan zerbitzuaren ukapen egoera sortu edo informazio sentikorra eskuratu.

Konponbidea:

Fuji Electric-ek ahultasun horiek konpontzen dituen firmwarearen 4.0.4.0 bertsioa argitaratu du. Lotura honetan dago eskuragarri:

http://monitouch.fujielectric.com/site/support-e/download-index-01.html

Xehetasuna:

- Erasotzaile batek kodea urrunetik exekutatzea lor lezake bereziki diseinatutako fitxategi bat erabiliz, eta ondorioz bufferraren gainezkatzea eragingo luke. Ahultasun horretarako CVE-2018-10637 identifikatzailea erreserbatu da.
- Erasotzaile batek urrunetik kodea exekutatzea lor lezake fidagarria ez den erakuslearen deserreferentzia bidez. Ahultasun horretarako CVE-2018-14811 identifikatzailea erreserbatu da.
- Heap-ean oinarritutako bufferraren gainezkatzearen bidez erasotzaile batek kode ez fidagarria exekutatzea lor lezake. Ahultasun horretarako CVE-2018-14813 identifikatzailea erreserbatu da.
- Mugez kanpoko idazketa erako hainbat ahultasun baliatuz, erasotzaile batek urrunetik kodea exekutatzea lor lezake. Ahultasun horretarako CVE-2018-14815 identifikatzailea erreserbatu da.
- Erasotzaile batek kodea urrunetik exekutatzea lor lezake osokoen gainezkatze erako ahultasun bat baliatuz. Ahultasun horretarako CVE-2018-14817 identifikatzailea erreserbatu da.
- Mugez kanpoko irakurketa erako ahultasun bat baliatuz, erasotzaile batek kodea urrunetik exekutatzea lor lezake. Ahultasun horretarako CVE-2018-14819 identifikatzailea erreserbatu da.
- Pilan oinarritutako bufferraren gainezkatzea baliatuz erasotzaile batek urrunetik kodea exekuta lezake. Ahultasun horretarako CVE-2018-14823 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Siemensen produktuetan

Argitalpen data: 2018/09/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- TD Keypad Designer, bertsio guztiak
- SIMATIC WinCC OA, 3.14 eta lehenagoko bertsioak
- SCALANCE X300, 4.0.0 bertsioa baino lehenagoko guztiak
- SCALANCE X408, 4.0.0 bertsioa baino lehenagoko guztiak
- SCALANCE X414, bertsio guztiak

Azalpena:

Siemensek bere produktuei eragiten dieten hainbat ahultasun identifikatu ditu. Horiek baliatuz urruneko erasotzaile batek pribilegioak eskalatzea edo zerbitzuaren ukapen egoera sortzea lor lezake.

Konponbidea:

Siemensek hainbat konponbideren berri eman du, kaltetutako gailuaren arabera.

- TD Keypad Designer: TD proiektuak dituzten direktorioetan idazteko ahalmena soilik erabiltzaile baimenduei ematea eta TD proiektu fidagarriak soilik irekitzea.
- SIMATIC WinCC OA: v3.14-P021 bertsiora eguneratzea, hemen eskuragarri: https://portal.etm.at/index.php?option=com_content&view=category&id=67&layout=blog&Itemid=80
- SCALANCE X300 eta X400: 4.1.2 bertsiora eguneratzea, hemen eskuragarri, hurrenez hurren: https://support.industry.siemens.com/cs/us/en/view/109753720 eta https://support.industry.siemens.com/cs/us/en/view/109753720.
- SCALANCE X414: 443/TCP atakan integratutako web zerbitzarirako sarbidea neurri egokiekin babestea eta atakarako sarbidea soilik IP fidagarriei baimentzea. IP fidagarrietatik kaltetutako ekipoetara ahultasunak eskaneatzeko tresnen exekuzioa ekiditea.

Xehetasuna:

- SIEMENS TD Keypad Designer gailuak DLLren bahiketa erako ahultasuna dauka. Hori baliatuz erasotzaile batek kodea exekuta lezake aplikazioa erabiltzen ari den erabiltzailearen baimenekin. Erasotzaileak idazketa baimenak izan behar ditu TDren proiektuen direktorioaren gainean, eta erabiltzaile legitimo batek erasotzailearen proiektua erabili beharra dauka. Ahultasun horretarako CVE-2018-13806 identifikatzailea erreserbatu da.
- 5678/TCP atakarako sarbidea ez dago modu egokian kontrolatuta. Horren ondorioz, autentifikaziorik gabeko urruneko erasotzaile batek pribilegioen eskalatzea lor lezake SIMATIC WinCC OAn. Ahultasun horretarako CVE-2018-13799 identifikatzailea erreserbatu da.
- Erasotzaile batek 443/TCP atakan argitaratutako web interfazea balia lezake zerbitzuaren ukapena eragiteko, web zerbitzarira bereziki manipulatutako eskaerak bidaliz. SCALANCE gailua automatikoki berrabiatzen da, sarearen eskuragarritasunari eraginez. Ahultasun horretarako CVE-2018-13807 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Siemens, Ahultasuna

Pribilegioen kudeaketa desegokia Honeywell-en Android gailu mugikorretan

Argitalpen data: 2018/09/14

Garrantzia: Handia

Kaltetutako baliabideak:

- CT60, CN80 eta CT40, Android OS 7.1 exekutatzean
- CK75, CN51, CN75, CN75e, CT50 eta D75e, Android OS 6.0 exekutatzean
- CT50, EDA50k eta D75e, Android OS 4.4 exekutatzean
- EDA50, EDA50k, EDA70 eta EDA60k, Android OS 7.1 exekutatzean
- EDA51, Android OS 8.1 exekutatzean

Azalpena:

Google-en Android Team-ek eta Honeywellek pribilegioen kudeaketa desegokiko ahultasun bat aurkitu dute Android sistema eragilea erabiltzen duten Honeywell-en hainbat gailu mugikorretan. Erasotzaile batek aplikazio gaizto bat erabil lezake pribilegioen igoera lortzeko.

Konponbidea:

- CT60, Android OS 7.1 exekutatzean - (GMS bertsioa) Android OS 84.00.11 bertsiora edo berriagora eguneratzea; (ez GMS bertsioa) Android 83.00.11 bertsiora edo berriagora eguneratzea
- CN80, Android OS 7.1 exekutatzean - (GMS bertsioa) Android OS 84.00.11 bertsiora edo berriagora eguneratzea; (ez GMS bertsioa) Android 83.00.11 bertsiora edo berriagora eguneratzea
- CT40, Android OS 7.1 exekutatzean - (GMS bertsioa) Android OS 84.00.11 bertsiora edo berriagora eguneratzea; (ez GMS bertsioa) Android 83.00.11 bertsiora edo berriagora eguneratzea
- CK75, Android OS 6.0 exekutatzean - CommonES 4.02.00.4082 bertsiora edo berriagora eguneratzea; ECP eguneratzea 2.30.00.0167 bertsiora edo berriagora (aplikagarria bada)
- CN75, Android OS 6.0 exekutatzean - CommonES 4.02.00.4082 bertsiora edo berriagora eguneratzea; ECP eguneratzea 2.30.00.0167 bertsiora edo berriagora (aplikagarria bada)
- CN75e, Android OS 6.0 exekutatzean - CommonES 4.02.00.4082 bertsiora edo berriagora eguneratzea; ECP eguneratzea 2.30.00.0167 bertsiora edo berriagora (aplikagarria bada)
- CT50, Android OS 6.0 exekutatzean - CommonES 4.01.00.4134 bertsiora edo berriagora eguneratzea; ECP eguneratzea 2.30.00.0167 bertsiora edo berriagora (aplikagarria bada)
- D75e, Android OS 6.0 exekutatzean - CommonES 4.01.00.4134 bertsiora edo berriagora eguneratzea; ECP eguneratzea 2.30.00.0167 bertsiora edo berriagora (aplikagarria bada)
- CT50, Android OS 4.4 exekutatzean - CommonES 3.17.3445 edo berriagora eguneratzea
- D75e, Android OS 4.4 exekutatzean - CommonES 3.17.3445 edo berriagora eguneratzea
- CN51, Android OS 6.0 exekutatzean - CommonES 4.01.03.3992 bertsiora edo berriagora eguneratzea; ECP eguneratzea

2.30.00.0167 bertsiora edo berriagora (aplikagarria bada)
- EDA50k, Android OS 4.4 exekutatzean - CommonES 3.17.3321.10 edo berriagora eguneratzea, data honetan eskuragarri: 2018/9/21
- EDA50, Android OS 7.1 exekutatzean - CommonES 5.01.01.4217 edo berriagora eguneratzea, data honetan eskuragarri: 2018/9/17
- EDA50k, Android OS 7.1 exekutatzean - CommonES 5.01.01.4217 edo berriagora eguneratzea, data honetan eskuragarri: 2018/9/17
- EDA70, Android OS 7.1 exekutatzean - CommonES 5.01.01.4217 edo berriagora eguneratzea, data honetan eskuragarri: 2018/9/17
- EDA60k, Android OS 7.1 exekutatzean - (ez GMS) Android 206.01.00.0018 bertsiora edo berriagora eguneratzea; ECP eguneratzea 2.30.00.0167 bertsiora edo berriagora, data honetan eskuragarri: 2018/9/17
- EDA51, Android OS 8.1 exekutatzean - CommonES 6.02.01.4593ra eguneratzea, data honetan eskuragarri: 2018/9/17

Xehetasuna:

Helburuari buruzko ezagupen aurreratuak lituzkeen erasotzaile batek sistema engainatzeko moduko aplikazio bat sor lezake eta bertan pribilegio altuak lortu. Horri esker erasotzaileak sarbidea lortuko luke honakoetara: pasahitzak, informazio pertsonala, argazkiak, emailak eta bestelako dokumentuak. Ahultasun horretarako CVE-2018-14825 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Mugikorrak, Ahultasuna

Hainbat ahultasun Wecon-en PLC Editor-en

Argitalpen data: 2018/09/18

Garrantzia: Ertaina

Kaltetutako baliabideak:

- PLC Editor, bertsio guztiak.

Azalpena:

Zero Day Initiativeko Natnael Samson (Natti) ikertzaileak bufferraren gainezkatze erako ahultasun hauen berri eman du. Ahultasun horiek arrakastaz baliatuz gero, erasotzaile batek urrunetik kodea exekuta lezake kaltetutako produktuan.

Konponbidea:

Ahultasunaren izaera dela eta, arintze posible bakarra da aplikazioaren interakzioa fitxategi fidagarrien artekoa soilik izan dadin baimentzea.

Xehetasuna:

- Bufferraren gainezkatze erako bi ahultasun baliatuz, erasotzaile batek urruneko kodea exekuta lezake Wecon PLC Editor-en softwarearen instalazioan. Erabiltzailearen interakzioa behar da ahultasun hau baliatzeko, orrialde bat bisitatu behar baitu edo fitxategi gaizto bat ireki. Arazoa WCP fitxategien barnean dago. ProjectVersion elementua edo DevCmt aztertzean, prozesuak ez du zuzen balioztatzen erabiltzaileak emandako datuen luzera, tamaina finkoko bufferrean kopiatu aurretik. Erasotzaileak ahultasun hau balia lezake kodea exekutatzeko indarrean dagoen prozesuan.

Etiketak: 0day, Ahultasuna

Autentifikaziorik eza Tec4Data-ren SmartCooler-en

Argitalpen data: 2018/09/21

Garrantzia: Ertaina

Kaltetutako baliabideak:

- SmartCooler, firmwarearen 180806 bertsioa baino lehenagoko guztiak.

Azalpena:

NewSky Securityko Ankit Anubhav ikertzaileak eman du Tec4Datako SmartCooler-ek duen autentifikaziorik eza erako ahultasun baten berri. Hori baliatuz urruneko erasotzaile batek zerbitzuaren ukapen egoera eragin lezake.

Konponbidea:

Fabrikatzaileak ahultasun hori konpontzeko firmwarearen bertsio berri bat garatu du eta kaltetutako gailuetara zabaldu du.

Xehetasuna:

- Gailuak autentifikaziorik gabeko urruneko berrabiatze komando bati erantzuten dio eta hori erasotzaile batek balia lezake zerbitzuaren ukapena eragiteko. Ahultasun horretarako CVE-2018-14796 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna

Hainbat ahultasun Rockwell Automation-en RSLinx Classic-en

Argitalpen data: 2018/09/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- RSLinx Classic, 4.00.01 bertsioa eta lehenagokoak.

Azalpena:

Rockwell Automationek, Tenable eta Nozomi Networks-eko Younes Dragonirekin lankidetzan, bufferraren gainezkatze eta baliabideen kontrolik gabeko kontsumo erako hainbat ahultasunen berri eman dute. Ahultasun horiek arrakastaz baliatuz gero, kaltetutako gailurako sarbidea blokea liteke edo bertan kodea exekutatu.

Konponbidea:

- Rockwell Automationek ahultasun horiek arintzen dituen softwarearen bertsio berri bat argitaratu du. Bertsio berri hori bere plataformatik deskarga daiteke, aldez aurretik erregistratu ondoren, ondoko loturan:
  - https://rockwellautomation.custhelp.com/app/answers/detail/a_id/1075712
- Rockwell Automationek 44818/tcp ataka desgaitzea ere aholkatzen du, posible baldin bada behintzat komunikazio horiek erabiltzen ari ez badira.

Xehetasuna:

- Bufferraren gainezkatze erako ahultasun bat baliatuz, urruneko erasotzaile batek gaizki sortutako CIP pakete bat bidal lezake 44818 atakara, eta horrek software aplikazioak ez erantzutea eta hura gelditzea eragingo luke. Gainera, ahultasun hori baliatuz urrunetik kodea exekutatu ere egin liteke, bufferraren gainezkatzeari esker. Ahultasun horretarako CVE-2018-14829 identifikatzailea erreserbatu da.
- Bufferraren gainezkatze erako ahultasun bat baliatuz, autentifikaziorik gabeko urruneko erasotzaile batek gaizki sortutako CIP pakete bat bidal lezake 44818 atakara, RSLinx-en Classic aplikazioan zerbitzuaren ukapen egoerak sortzeko xedearekin. Erabiltzaileak softwarea eskuz berrabiarazi beharko du berriro modu egokian funtziona dezan. Ahultasun horretarako CVE-2018-14821 identifikatzailea erreserbatu da.
- Autentifikaziorik gabeko urruneko erasotzaile batek bereziki diseinatutako Ethernet/IP paketeak bidal litzake 44818 atakara. Hori eginez aplikazioak erantzuteari uztea eta gelditzea eragingo du, baliabideen kontrolik gabeko kontsumo bat dela eta. Erabiltzaileak softwarea berrabiarazi beharko du funtzionaltasuna berreskuratzeko. Ahultasun horretarako CVE-2018-14827 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Zerbitzu ukapena Phoenix Contact-en AXL F BK PN-n

Argitalpen data: 2018/09/24

Garrantzia: Handia

Kaltetutako baliabideak:

- AXL F BK PN, 1.0.4 bertsioa eta lehenagokoak
- AXL F BK ETH, 1.12 bertsioa eta lehenagokoak
- AXL F BK ETH XC, 1.11 bertsioa eta lehenagokoak

Azalpena:

Fraunhofer IOSBeko Anne Borcherding, Steffen Pfrang, David Meier eta Christian Haas ikertzaileek zerbitzuaren ukapen erako ahultasun baten berri eman dute, Phoenix Contacten AXL F BK PN produktuei eragiten diena. Hori baliatuz autentifikaziorik gabeko urruneko erasotzaile batek busaren akoplagailuan erabateko blokeoa abia lezake.

Konponbidea:

Phoenix Contactek ez dauka ahultasun hau konpontzeko inolako eguneraketarik edo firmware berririk.

Beren babeserako, Phoenix Contactek bere bezeroei aholkatzen die gailuak sare itxietan edo suebaki egokiez babesturik erabiltzea. Informazio gehiago hemen eskura daiteke:
https://www.phoenixcontact.com/assets/downloads_ed/local_pc/web_dwl_technical_info/ah_en_industrial_security_107913_en_01.pdf

Xehetasuna:

- Gailuak erantzuteari uzten dio edozein sare edo ataka lokalen aurrean eta ondorioz itxi edo itzali egiten da automatizazio sistemaren zati hori. Bus akoplagailua berrabiarazi beharra dago indarra deskonektatuz. Ahultasun horretarako CVE-2018-16994 identifikatzailea erabili da.

Etiketak: Ahultasuna

Hainbat ahultasun Fuji Electric-en Alpha5 eta Frenic Loader-en

Argitalpen data: 2018/09/27

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Alpha5 Loader
- Frenic Loader

Azalpena:

Zero Day Initiativeko Michael Flandersek eta Ghirmay Destak bufferraren gainezkatze eta mugez kanpoko irakurketa erako hainbat ahultasunen berri eman dute, Fuji Electric-en Alpha5 eta Frenic Loader produktuei eragiten dietenak. Erasotzaile batek kodea exekuta lezake urrunetik edo informazio sentikorra eskuratu.

Konponbidea:

Ahultasunen izaera dela eta, arintze neurri posible bakarra da aplikazioaren interakzioa fitxategi fidagarrien artekoa soilik izan dadin baimentzea.

Xehetasuna:

Ahultasun horiek guztiek erabiltzailearen interakzioa behar dute baliatuak izan ahal izateko. Izan ere, beharrezkoa da asmo gaiztoko orrialde bat bisitatzea edo fitxategi gaizto bat irekitzea.

- Bufferrak gainezka egitea: Akatsa gertatzen da C5V, AP5 edo FNC fitxategiak prozesatzeko unean, erabiltzaileak emandako datuen luzeraren balioztatze falta dela eta, luzera finkoko buffer batera kopiatuak izan aurretik. Ahultasun hau baliatuz, erasotzaile batek kodea exekuta lezake urrunetik edo informazio pribilegiatua lortu.
- Mugez kanpoko irakurketa: Akatsa gertatzen da C5V, AP5 edo FNC fitxategiak prozesatzeko unean, erabiltzaileak emandako datuen luzeraren balioztatze falta dela eta. Ondorioz irakurketa esleitutako bufferretik kanpora egiten da. Erasotzaile batek instalazio ahulei buruzko informazio sentikorra eskura lezake

Etiketak: 0day, Ahultasuna

Hainbat ahultasun Yokogawa-ren STARDOM kontrolagailuetan

Argitalpen data: 2018/09/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- FCN-500, R4.10 bertsioa eta lehenagokoak.
- FCN-RTU, R4.10 bertsioa eta lehenagokoak.
- FCN-100, FCJ, R4.10 bertsioa eta lehenagokoak.

Azalpena:

Yokogawak jakinarazi duenez bere STARDOM kontrolagailuek hainbat ahultasun dituzte, era ezberdinetakoak: kredentzialen kudeaketa desegokia, zerbitzuaren ukapena, pasahitz barneratuak eta memoria ahitzea. Erasotzaile batek ahultasun horiek balia litzake zerbitzuaren ukapen egoera sortzeko, memoria ahitzeko edo kaltetutako gailuetatik kredentzialak eskuratzeko.

Konponbidea:

Memoria ahitzearen ahultasuna konpontzeko Yokogawak aholkatzen du softwarea R4.20 bertsiora eguneratzea.

Gainerako ahultasunei dagokienez, FCN paketeen iragazki funtzioa erabiltzea gomendatzen da eta hori konfiguratzea konfiantzako jatorria duten komunikazioak soilik baimentzeko. Gainera, sarean segurtasun neurriak hartzea gomendatzen da, konfiantzakoak ez diren hirugarren pertsonek komunikazio datuak ezin harrapa ditzaten.

Xehetasuna:

- Erasotzaile batek kredentzialak lor litzake kontrolagailuetara urruneko sarbidea lortzeko, kredentzialak modu desegokian kudeatzen direnez gero.
- Erasotzaile batek kontrolagailuak urrunetik kudeatzeko funtziorako sarbidearen ukapena eragin dezake.
- Barneratutako pasahitzak erabiltzearen ondorioz, erasotzaile batek saioa has lezake kontrolagailuaren mantenu funtzioan eta informazioa eskuratu edo hura manipulatu. Eraso hori soilik egin daiteke gailua mantenu egoeran dagoenean.
- Erasotzaile batek memoria ahitzea eragin dezake, kontrolagailuen zerbitzura baimendu gabeko HTTP eskaera bat bidaliz.

Etiketak: Ahultasuna

Hainbat ahultasun Emerson-en AMS Device Manager-en

Argitalpen data: 2018/09/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- AMS Device Manager, 12.0tik 13.5era bitarteko bertsioak

Azalpena:

Kaspersky Lab-eko Sergy Temnikov ikertzaileak, Emersonekin lankidetzan, pribilegioen kudeaketa eta sarbide kontrol okerreko hainbat ahultasunen berri eman du.

Konponbidea:

Emersonek erabiltzaileei aholkatzen die 12.0 bertsioa duten kaltetutako produktuak 13.5era eguneratzea. Erabiltzaileentzako partxeak hemen daude eskuragarri:

https://guardian.emersonprocess.com/

CVE-2018-14808 ahultasuna ezingo litzateke baliatu aplikazioen zerrenda zuri bat ezarriko balitz, fitxategiak gainidaztea saihestuko bailuke.

Ahultasun horren eta beste batzuen eragina murrizteko, Emerson-ek gomendatzen du AMS Device Manager ezartzea eta konfiguratzea, AMS Device Manager-en gidan azalduta dagoen moduan, Emerson Guardian-en zerbitzu atarian eskuragarri dagoena.

Xehetasuna:

- Urruneko erasotzaile batek bereziki diseinatutako script bat erabil lezake kaltetutako softwarean kode arbitrarioa exekutatzeko, sarbide kontrol desegoki baten ondorioz. Ahultasun horretarako CVE-2018-14804 identifikatzailea erabili da.
- Administratzaileak ez diren erabiltzaileek kaltetutako softwarearen fitxategi exekutagarriak eta liburutegiak alda ditzakete, pribilegioen kudeaketa desegoki bat baliatuz. Ahultasun horretarako CVE-2018-14808 identifikatzailea erabili da.

Etiketak: Ahultasuna

Mugez kanpoko irakurketa Delta Electronics-en Delta Industrial Automation PMSoft-en

Argitalpen data: 2018/09/28

Garrantzia: Ertaina

Kaltetutako baliabideak:

- Delta Industrial Automation PMSoft v2.11 edo lehenagokoak.

Azalpena:

Zero Day Initiativeko Mat Powell ikertzaileak eman du mugez kanpoko irakurketa erako ahultasun honen berri. Arrakastaz baliatuz gero urruneko erasotzaile batek informazio konfidentziala irakur lezake.

Konponbidea:

- Delta Electronics-ek kaltetutako bezeroei aholkatzen die PMSoft (v2.12) softwarearen azken bertsiora eguneratzea, 2018ko irailaren 18az geroztik eskuragarri dagoena, edo bestela eskuragarri dauden ondoreneko bertsioetara eguneratzea.

Xehetasuna:

- PPM fitxategien maneiatzaileak modu desegokian balioztatzen ditu erabiltzaileak emandako datuak. Hori baliatuz urruneko erasotzaile batek bufferrari esleitu zaizkion mugetatik harago irakurketak egin litzake. Ondorioz informazio konfidentziala irakur liteke edo ahultasun hori beste eraso teknika batzuekin batera erabil liteke kode gaiztoa exekutatzeko. Ahultasun horretarako CVE-2018-14824 identifikatzailea erabili da.

Etiketak: Edukien kudeatzailea, Pribatutasuna, Ahultasuna