2018ko Maiatzaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Hainbat ahultasun Siemensen produktuetan

Argitaratze-data: 2018/05/03

Garrantzia: Handia

Kaltetutako baliabideak:

- Siveillance VMS 2016 R eta aurrekoak, V10.0a bertsioaren aurreko guztiak.
- Siveillance VMS 2016 R2, V10.1a bertsioaren aurreko guztiak.
- Siveillance VMS 2016 R3, V10.2b bertsioaren aurreko guztiak.
- Siveillance VMS 2017 R1, V11.1a bertsioaren aurreko guztiak.
- Siveillance VMS 2017 R2, V11.2a bertsioaren aurreko guztiak.
- Siveillance VMS 2018 R1, V12.1a bertsioaren aurreko guztiak.
- Siveillance VMS Video Android eta IOSerako, V12.1a (2018 R1) bertsioaren aurreko guztiak.
- SINAMICS GH150 V4.7 w. PROFINET, V4.7 SP5 HF7 bertsioaren aurreko guztiak.
- SINAMICS GH150 V4.7 w. PROFINET, V4.7 HF30 bertsioaren aurreko guztiak.
- SINAMICS GL150 V4.7 w. PROFINET, SINAMICS GM150 V4.7 w. PROFINET, SINAMICS SL150 V4.7.4 w. PROFINET, SINAMICS SL150 V4.7.5 w. PROFINET eta SINAMICS SM120 V4.7 w. PROFINET. V4.8 SP2 bertsioaren aurreko guztiak.
- SINAMICS SM150 V4.7 w. SIMOTION eta PROFINET. Bertsio guztiak.

Azalpena:

TZI Bremen Karsten Sohr ikertzaileak Android eta IOSerako Siveillance VMS Video Mobile App produktuarekin erlazionatutako ahultasun batzuk atzeman ditu. Horien ondorioz, erasotzaile batek datuak irakurri edo idatz litzake, App eta zerbitzariaren arteko komunikazio-kanal bidean. SINAMICS eta Siveillance VMS sistemei eragiten dieten gainerako ahultasunen ondorioz, erasotzaile batek pribilejioak igotzea edota Zerbitzua Ukatzea eragin dezake.

Konponbidea:

Siemens etxeak software egokitzapenak burutu ditu, produktuei eragiten dieten ahultasunak konpontzeko. Ondoren, produktuak eta dagozkien eguneratzeak zerrendatuko dira:

- Siveillance VMS 2016 R eta aurrekoak ? 10.0a bertsiora eguneratzea.
- Siveillance VMS 2016 R2 ? 10.1a bertsiora eguneratzea.
- Siveillance VMS 2016 R3 ? V10.2b bertsiora eguneratzea.
- Siveillance VMS 2017 R1 ? V11.1a bertsiora eguneratzea.
- Siveillance VMS 2017 R2 ? V11.2a bertsiora eguneratzea.
- Siveillance VMS 2018 R1 ? V12.1a bertsiora eguneratzea.

Bisitatu honako lotura, produktuari dagokion eguneraketa deskargatzeko: https://psp.sbt.siemens.com/

Gainera, aplikatu beharreko gomendio nagusi moduan, fabrikatzaileak gomendatzen du 7474/TCP zubietatik eta 9993/TCP zubitik sare bidezko sarbidea mugatzeko, Siveillance VMS produktuei.

- Siveillance VMS Video Android eta iOSerako: V12.1a (2018 R1) bertsiora eguneratzea (https://play.google.com/store/apps/details?id=com.siemens.siveillancevms, https://itunes.apple.com/us/app/siveillance-vms-video/id1045047239)
- SINAMICS GH150 V4.7 w. PROFINET eta SINAMICS SL150 V4.7.0 w. PROFINET: V4.7 SP5 HF7 bertsiora eguneratzea edo V4.8 SP2 bertsiora aldatzea.
- SINAMICS GL150 V4.7 w. PROFINET, SINAMICS GM150 V4.7 w. PROFINET, SINAMICS SL150 V4.7.4 w. PROFINET, SINAMICS SL150 V4.7.5 w. PROFINET eta SINAMICS SM120 V4.7 w. PROFINET: V4.8 SP2 bertsiora eguneratzea.
- SINAMICS SM150 V4.7 w. SIMOTION eta PROFINET.
  - Sareko babesa aplikatzea eta defentsa sakon ezartzea.
  - 161/TCP portutik sare bidezko sarbidea babestea.
  - VPN zerbitzuen erabilera, sareen arteko komunikazioak babesteko.

Xehetasuna:

- Pribilejioen eskalatzea edota zerbitzuaren ukapena Siveillance VMS produktuan: Siemensen Siveillance VMS software batzuek ahultasun bat dute, okerreko deserializazio baten ondorioz. Bertako erasotzaile batek ahultasun hori erabil dezake pribilejioak igo edota zerbitzua ukatzeko. Ahultasun horretarako CVE-2018-7891 kode bat erreserbatu da.
- Zerbitzua ukatzea SINAMICS produktuan: Tokiko sareko erasotzaile batek broadcast PROFINET paketeak bidal litzake, bereziki

manipulatuta, eragindako produktuen gaineko zerbitzu ukapena eraginez. Eragile bat behar da sistema berreskuratzeko. Ahultasun horretarako CVE-2017-2680 identifikatzailea erreserbatu da.
- Zerbitzua ukatzea SINAMICS produktuan: Tokiko sareko erasotzaile batek paketeak bidal litzake 161/UDP portura, bereziki manipulatuta, eragindako produktuen gaineko zerbitzu ukapena eraginez. Kaltetutako produktuak eskuz berrabiarazi behar dira. Ahultasun horretarako CVE-2017-12741 identifikatzailea erreserbatu da.Informazioa zabaltzea Siveillance VMS Video Mobile App produktuan: Ziurtagiri bat okerreko moduan balioztatzearen ondorioz, erasotzaile batek datu zifratuen kanalean datuak irakurri eta idatz litzake, zerbitzariaren eta aplikazioaren artean, Man-in-the-Middle motako eraso baten bidez komunikazio bat jaso edota balioztatze algoritmo baten ondoriozko ziurtagiri bat sortu, onartuaren modukoa. Ahultasun horretarako, CVE-2018-4849 identifikatzailea erreserbatu da.

Etiketak: iOS, Mugikorrak, Siemens, Ahultasuna

Hainbat ahultasun Lantech-en IDS 2012 sisteman

Argitaratze-data: 2018/05/04

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- IDS 2012 bertsioa 2.0 eta aurrekoak.

Azalpena:

Florian Adamsky ikertzaileak Lantech-en IDS 2012 produktuari eragiten dioten hainbat ahultasun atzeman ditu. Urrutiko erasotzaile batek ahultasun horiek baliatu litzake sisteman urrutiko kodea exekutatzeko, sarrerako eremuen okerreko balioztatze baten ondorioz.

Konponbidea:

Lantech-ek ez du ahultasun horietarako konponbiderik eman.

Xehetasuna:

- Sarrera-datuak oker balioztatzea: Kaltetutako produktuaren sarrera-eremu gehienek ez dute balioztatze zuzenik. CVE-2018-8869 kodea esleitu zaio ahultasun horri.
- Bufferrak gainezka egitea. Erasotzaile batek kodea urrutitik exekuta lezake. CVE-2018-8865 kodea esleitu zaio ahultasun horri.

Etiketak: Ahultasuna

Hainbat ahultasun Philips markako Brilliance CT eskanerretan

Argitaratze-data: 2018/05/04

Garrantzia: Handia

Kaltetutako baliabideak:

- Brilliance 64 2.6.2 bertsioa eta aurrekoak
- Brilliance iCT 4.1.6 bertsioa eta aurrekoak
- Brillance iCT SP 3.2.4 bertsioa eta aurrekoak.
- Brilliance CT Big Bore 2.3.5 bertsioak eta aurrekoak.

Azalpena:

Philipsek 3 ahultasunen berri eman du; horietako bat larritasun altukoa, beharrezko ez diren pribilejioekin exekutatzen den, baliabideak erakusten dituen eta kredentzial barneratuak erabiltzen dituen motakoa. Tomografia konputerizatuak egiteko Brilliance eskanerrei eragiten diete eta erasotzaile batek aukera eduki lezake kaltetutako sistemen konfidentzialtasun, osotasun eta eskuragarritasunean eragiteko.

Konponbidea:

Philips etxeak arriskuak murriztu eta kontrolatzeko honako gida identifikatu du:

- Erabiltzaileek Philips etxearen Brilliance CT produktu guztiak erabili behar dituzte Philipsek baimendutako azalpenen arabera, Philipsek berak onartutako softwarearen konfigurazioa, sistemaren zerbitzuak eta segurtasun konfigurazioa barne, baita suebakien eragiketak ere.
- Philipsek defentsarako estrategia sakon bat ezartzeko eskatzen die erabiltzaileei, beren sistemak barne eta kanpo segurtasun mehatxuen aurka babesteko. Horren barruan, baimena duten langileek soilik erabiliko lukete eskanerra, baimenik gabeko erabiltzaileren baten erabilerak saiheste aldera.

Philipsek kredentzial barneratuen ahultasunak ere konpondu ditu, Brilliance iCT 4.x eta aurreko bertsioetarako. Phil iCT-iPatient (v4.x) familiaren erabilerarako jarraibideetan kredentzialak administratzeari buruz hitz egiten da eta Philips InCenter delakotik sar daiteke, eskubideak dituzten erabiltzaileentzako https://incenter.medical.philips.com gunean.

Xehetasuna:

- Behar ez diren pribilejioekin aritzea: Kaltetutako gailuak erabiltzailearen funtzioekin ari dira, Microsoft Windows sistema eragile batean jasotako kiosko baten bidez. Windows pribilejio altuekin hasten da, berez. Horri esker, erasotzaile, aplikazio edo erabiltzaile batek baimenik gabeko pribilegio altuak lor litzake. Gainera, erasotzaileek Windowsen baliabide ez baimenduetarako sarbidea izan dezakete. Ahultasun horretarako CVE-2018-8853 identifikatzailea erreserbatu da.
- Baliabideak agerian jartzea: Sarbide mugatua duen erabiltzaile bat edo baimenik gabeko erasotzaile bat kioskoaren euste-eremutik irten liteke, sistemaren pribilejio altuak lortu eta sistema eragilearen barruan baimenik gabeko baliabideetarako sarbidea izan. Ahultasun horretarako CVE-2018-8861 identifikatzailea erreserbatu da.
- Kredentzial barneratuen erabilera: Softwareak kredentzial finkoak ditu, hala nola pasahitz edo gako kriptografikoak, sarbidea egiaztatzeko, kanpo osagaiei irteeraren berri emateko edo barne datuak zifratzeko erabiltzen duena. Erasotzaile batek kredentzial

horiek konprometitu litzake eta sistemara sartzea lortu. Ahultasun horretarako CVE-2018-8857 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna

Hainbat ahultasun atzeman dira Silex Technology eta GE Healthcare produktu batzuetan

Argitaratze-data: 2018/05/09

Garrantzia: Handia

Kaltetutako baliabideak:

- GEH-500 1.54 bertsioa eta aurrekoak
- SX-500 bertsio guztiak. (ez jarraitua 2011tik)
- GEH-SD-320AN GEH-1.1 bertsioa eta aurrekoak
- SD-320AN 2.01 bertsioa eta aurrekoak (ez jarraitua 2017ko azarotik)
- GE MAC Resting ECG MAC 3500 eredua
- GE MAC Resting ECG MAC 5000 eredua. (Ez jarraitua 2012tik)
- GE MAC Resting ECG MAC 5500 eredua
- GE MAC Resting ECG MAC HD 5500 eredua

Azalpena:

Atredis Partners enpresako Eric Evenchick ikertzaileak hainbat ahultasun atzeman ditu, Silex Technology eta GE Healthcare produktuei eragiten dietenak. Urrutiko erasotzaile batek aukera edukiko luke, ahultasun horiek baliatuz, sistemaren konfigurazioa aldatzeko edo kodea urrutitik exekutatzeko.

Konponbidea:

Silex Technology eta GE Healthcare enpresek honako neurriak hartzea gomendatu dute:

- CVE-2018-6020 (GE MobileLink/SX-500): ?Update? kontua gaitzea web interfazean, berez desgaituta datorrena. ?Update? kontu horretan bigarren pasahitz bat konfiguratzea, gailuan egiaztatu gabeko konfigurazio aldaketak prebenitzeko.
- CVE-2018-6021 (GE MobileLink/GEH-SD-320AN): Silex Technology eta GE Healthcare enpresek eguneraketa bat garatu dute ahultasuna konpontzeko. Deskargatzeko moduan egongo da, behin testatuta, 2018ko maiatzaren 31tik aurrera.

Xehetasuna:

- Egiaztatze okerra: Sisteman egiaztatzea ez da behar den moduan bermatzen POST eskaera batzuetarako. Hori dela eta, erasotzaile batek sistemaren konfigurazio batzuk aldatu litzake. CVE-2018-6020 kodea esleitu zaio ahultasun horri.
- Parametroen balioztatze okerra sistemarako deietan: Sistemarako deietan erabilitako parametroak ez dira behar den moduan sanitizatu; horren ondorioz, erasotzaile batek kodea exekutatu lezake, parametro horietan komandoak injektatuz. CVE-2018-6021 kodea esleitu zaio ahultasun horri.

Etiketak: Ahultasuna

Kontrol falta fitxategi edo direktorioetarako sarbidean MatrikonOPren MatrikonOPC Explorer-en

Argitalpen data: 2018/05/11

Garrantzia: Ertaina

Kaltetutako baliabideak:

- MatrikonOPC Explorer, 5.0 eta lehenagoko bertsioak

Azalpena:

Positive Technologies-eko Ilya Kapov ikerlariak fitxategi edo direktorioetarako sarbidean kontrol faltarekin zerikusia duen ahultasun honen berri eman du. Sistemara sarbide lokala lukeen erasotzaile batek ahultasun hau balia lezake ostalaritik fitxategiak transferitzeko baimenik gabe. Horrek informazioa hedatzea eragin lezake.

Konponbidea:

MatrikonOPCk ahultasun hori konpontzen duen partxe bat argitaratu du. Ondorengo loturatik jaits daiteke partxea:

https://www.matrikonopc.com/downloads/176/software/index.aspx

Xehetasuna:

- Hirugarrenentzat eskuragarri dauden fitxategi edo direktorioen ahultasuna: Ahultasun hau arrakastaz baliatuz gero, sistemara sarbide lokala lukeen erasotzaile batek ostalaritik fitxategiak transferi litzake baimenik gabe. CVE-2018-8714 kodea esleitu zaio ahultasun horri.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Rockwell Automation-en produktuetan

Argitalpen data: 2018/05/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Arena, 15.10.00 bertsioa eta lehenagokoak
- FactoryTalk Activation Manager v4.00 eta v4.01, Wibu-Systems CodeMeter v6.50b eta lehenagoko bertsioetan zabaldua
- FactoryTalk Activation Manager v4.00 eta lehenagoko bertsioak, FlexNet Publisher v11.11.1.1 eta lehenagoko bertsioekin zabaldua
- Komeni da ohartaraztea ondoko produktuak FactoryTalk Activation Manager erabili beharrean daudela:
  - Arena
  - Emonitor
  - FactoryTalk AssetCentre
  - FactoryTalk Batch
  - FactoryTalk EnergyMetrix
  - FactoryTalk eProcedure
  - FactoryTalk Gateway
  - FactoryTalk Historian Classic
  - FactoryTalk Historian Site Edition (SE)
  - FactoryTalk Information Server
  - FactoryTalk Metrics
  - FactoryTalk Transaction Manager
  - FactoryTalk VantagePoint
  - FactoryTalk View Machine Edition (ME)
  - FactoryTalk View Site Edition (SE)
  - FactoryTalk ViewPoint
  - RSFieldBus
  - RSLinx Classic
  - RSLogix 500
  - RSLogix 5000
  - RSLogix5
  - RSLogix Emulate 5000
  - RSNetWorx
  - RSView32
  - SoftLogix 5800
  - Studio 5000 Architect
  - Studio 5000 Logix Designer
  - Studio 5000 Logix Emulate
  - Studio 5000 View Designer

Azalpena:

Rockwell Automation-ek eta Ariele Caltabiano ikerlariak, Trend Microko Zero Day Initiativerekin lankidetzan, hainbat ahultasun aurkitu dituzte. Horiek baliatuz, kaltetutako gailuetara sarbidea lukeen erasotzaile batek informazio sentikorra eskura lezake, edukia gainidatzi, zerbitzuaren ukapen egoera sortu edo bufferraren gainezkatzea eragin, eta agian baita urrunetik kodea exekutatu ere.

Konponbidea:

Factory Talk Activation Manager-ekin instalatuak izan diren CodeMeter edo FlexNet Publisher-en bertsio kaltetuak dituzten erabiltzaileei v4.02 bertsiora eguneratzea aholkatzen die Rockwell Automation-ek.Ez bada posible Factory Talk Activation Manager-en v4.02 bertsiora zuzenean eguneratzea, lehenbizi CodeMeter eguneratu beharko litzateke eguneraketa hura onartzen duen bertsio batera.

Arena Software-ren erabiltzaileek v15.10.01 eta ondoreneko bertsio eguneratuak dituzte eskuragarri, ahultasunak konpontzen dituztenak. Ondorengo lotura honetatik jaits daitezke (Sarbide pribatua):
https://rockwellautomation.custhelp.com/app/answers/detail/a_id/1073588

Eguneraketez gain, Rockwell Automationek beste segurtasun neurri osagarri batzuk ere ezartzea gomendatzen du:

- Ethernet/IP trafiko guztia edo CIPen oinarritutako beste protokolo batzuk blokeatzea, salbu eta guztiz beharrezkoa den kasuetan. Sarbide mugatua izan behar duten atakak ondoko hauek dira: TCP/2222 eta UDP/44818.Trafikoaren kontrolerako neurriak erabiltzea gomendatzen da, adibidez suebakiak, UTM eta abar.
- Gailuen agerpena murriztea eta Internetetik sarbiderik ez dutela bermatzea.
- Urruneko sarbideak metodo seguruekin egitea, adibidez VPNak (Virtual Private Networks) erabiliz.

Detalle:

- Cross-Site-Scripting ("XSS"): erasotzaile lokal batek Wibu-Systems CodeMeter-en ahultasuna balia lezake web scriptak edo HTML kodea injektatzeko, konfigurazio fitxategiko eremu bat baliatuz. Ahultasun horri esker erasotzaileak informazio sentikorra eskura lezake edo HTML orriaren edukia gainidatzi. CVE-2017-13754 kodea esleitu zaio ahultasun horri.
- Eragiketen murrizketa okerra bufferraren memoriaren mugen barnean: FlexNet Publisher-en barnean kateak kopiatzeko ardura duen funtzio pertsonalizatu batek ez ditu modu egokian baliozkotzen sarbide datuak. Hori baliatuz erasotzaile batek, autentifikaturik egon behar izan gabe, bereziki aldatutako mezuak bidal litzake bufferraren gainezkatzea eragitearren. CVE-2015-8277 kodea esleitu zaio ahultasun horri.
- Memoriaren askapen okerra: erasotzaile batek memoriaren erabilpena balia lezake, aldez aurretik modu zuzenean askatua izan ez bada, bereziki gaizki sortutako paketeak bidaltzeko, aplikazioari egoera ezegonkorra eraginez. Horrek gorde gabeko datuen erabilgarritasunari edo galerari eragin liezaioke. CVE-2018-8843 kodea esleitu zaio ahultasun horri.

Etiketak: Eguneraketa, Ahultasuna

Paketeen kudeaketa okerra Siemensen SIMATIC S7-400en

Argitalpen data: 2018/05/15

Garrantzia: Handia

Kaltetutako baliabideak:

- SIMATIC S7-400, hardwarearen 4.0 eta lehenagoko bertsioduna, bertsio guztiak
- SIMATIC S7-400, hardwarearen 5.0 bertsioduna, firmwarearen V5.2 bertsioa baino lehenagoko guztiak
- SIMATIC S7-400H, hardwarearen 4.5 eta lehenagoko bertsioduna, bertsio guztiak

Azalpena:

Siemensek gaizki osatutako paketeen kudeaketa okerraren ahultasun bat aurkitu du SIMATIC S7-400 gailuetan. Kaltetutako produktuan erasotzaile batek zerbitzuaren ukapen egoera eragin lezake.

Konponbidea:

Siemensek erabiltzaile guztiei honako bertsioetara eguneratzea aholkatzen die:

- SIMATIC S7-400, hardwarearen 4.0 eta lehenagoko bertsioduna: Hardwarearen 5.0 bertsiora eguneratzea, hemen eskuragarri: https://support.industry.siemens.com/cs/ww/en/view/109483507
- SIMATIC S7-400, hardwarearen 5.0 bertsioduna: Firmwarearen V5.2 edo goragoko bertsiora eguneratzea, hemen eskuragarri: https://support.industry.siemens.com/cs/ww/en/view/109474827
- SIMATIC S7-400H, hardwarearen 4.5 eta lehenagoko bertsioduna: Hardwarearen 6.0 bertsiora eguneratzea, hemen eskuragarri: https://support.industry.siemens.com/cs/ww/en/view/75407031

Xehetasuna:

Kaltetutako produktuek modu ezegokian baliozkotzen dituzte S7 komunikazio paketeak. Horrek zerbitzuaren ukapena eragin lezake, eta ondorioz eskuz berrabiarazi beharko litzateke. Erasotzaile batek bereziki gaizki osatutako S7 paketeak bidal litzake CPUaren komunikazio interfazera, Ethernet, PROFIBUS eta Multi Point Interfaces (MPI) interfazeetara barne. Ahultasun horretarako CVE-2018-4850 kodea erreserbatu da.

Etiketak: Eguneraketa, Siemens, Ahultasuna

Hainbat ahultasun Advantech-en WebAccess-en

Argitalpen data: 2018/05/16

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- WebAccess, 8.2_20170817 eta lehenagoko bertsioak
- WebAccess, 8.3.0 eta lehenagoko bertsioak
- WebAccess Dashboard, 2.0.15 eta lehenagoko bertsioak
- WebAccess Scada Node, 8.3.1 bertsioa baino lehenagokoak
- WebAccess/NMS, 2.0.3 eta lehenagoko bertsioak

Azalpena:

Trend Micro-ren Zero Day Initiative-rekin lanean diharduten ikerlari batzuek hainbat ahultasunen berri eman dute. Horiek baliatuz erasotzaile batek hostaren edota helburuaren informazio sentikorra heda lezake, kode arbitrarioa exekutatu edo fitxategiak ezabatu.

Konponbidea:

Advantechek ahultasun hau konpontzen duen partxe bat argitaratu du, hemen eskuragarri: http://support.advantech.com/support/DownloadSRDetail_New.aspx?SR_ID=1-MS9MJV&Doc_Source=Download

Xehetasuna:

Larritasun kritikoa duten ahultasunak honakoak dira:

- Baimentze okerra: TFTP aplikazio batek web aplikaziora mugarik gabeko fitxategien kargak ditu baimenik gabe, eta horrek erasotzaile bati kode arbitrarioa exekutatzea ahalbidetu liezaioke. Ahultasun horretarako CVE-2018-7505 identifikatzailea erabili da.
- Fitxategien bideen kudeaketa okerra: Fitxategien bideen kudeaketa okerreko ahultasun bat aurkitu da, eta horren bitartez erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2018-10589 identifikatzailea erabili da.
- Bufferrak gainezka egitea: Pilan oinarritutako bufferraren gainezkatzearen hainbat ahultasun aurkitu dira, eta horiek baliatuz erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2018-7499 identifikatzailea erabili da.
- Bufferrak gainezka egitea: Pilan oinarritutako bufferraren gainezkatzearen hainbat ahultasun aurkitu dira, eta horiek baliatuz erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2018-8845 identifikatzailea erabili da.
- Erreferentzia galdutako puntero ez fidagarria: Erreferentzia galdutako puntero ez fidagarrien hainbat ahultasun aurkitu dira, eta horiek baliatuz erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2018-7497 identifikatzailea erabili da.

Larritasun altu eta ertaineko gainerako ahultasunetarako erreserbatu diren kodeak honakoak dira: CVE-2018-10590, CVE-2018-7503, CVE-2018-7495, CVE-2018-884, CVE-2018-7501 eta CVE-2018-10591.

Etiketak: Eguneraketa, Ahultasuna

ABBren loturaren ateetako hainbat ahultasun

Argitaratze-data: 2018/05/16

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- IP-Gateway ? ABB Welcome System Device, 3,39 bertsioa eta aurrekoak
- IP-Gateway - Busch-Jaeger Systemgerät, 3,39 bertsioa eta aurrekoak

Azalpena:

ERNW enpresako Florian Grunow ikertzaileak, ICS-CERTen laguntzarekin, ahultasun horien berri eman dio ABB fabrikatzaileari. Ahultasun horiek baliatzekotan, erasotzaile batek gailuaren urrutiko kontrola lortu dezake eta kode arbitrarioa exekutatu.

Konponbidea:

ABB etxeak bezeroei gomendatu die argitaratu dituzten eguneratzeak egiteko (3.48 bertsioa eta ostekoak), ahultasunak konpontze aldera. Lotura honetan daude eskuragarri: http://www.busch-jaeger-catalogue.com/software.php

Xehetasuna:

- Urrutiko kodea injektatzea: Erasotzaile batek web bidezko lotura-atearen tokiko konfigurazioari eragiten dion ahultasun hori baliatu lezake. Bereziki diseinatutako paketeen bidalketari esker, erasotzaileak produktuaren kontrola lortu dezake eta kode arbitrarioa exekutatu. Kasu honetan, erasotzaileak sarerako sarbide zuzena izan behar du, gailuaren konfiguraziora web bidez sartzeko eta ahultasun hori baliatzeko. CVE-2017-7931 kodea esleitu zaio ahultasun horri.
- Saioko cookieen lapurreta: Administrari-pasahitza testu lau gisa gordetzen da, cookie baten bidez, baliozko saio-hasiera baten ostean. Erasotzaile batek gertaera hori baliatu lezake biktima baten nabigatzaileko cookiea hartu eta saioa lapurtzeko. Ahultasun hori baliatzeko, erasotzaileak bezeroaren sistema konprometitu behar du, lehenik. CVE-2017-7906 kodea esleitu zaio ahultasun horri.

Etiketak: Eguneratzea, Nabigatzailea, Ahultasuna

Hainbat ahultasun Phoenix Contact-en Switch FL tresnan

Argitaratze-data: 2018/05/17

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Switches FL 3xxx, 4xxx, 48xx ereduak, 1.0tik 1.33ra bitarteko firmware bertsioarekin.

Azalpena:

Positive Technologies enpresako Vyacheslav Moskvin, Semen Sokolov, Evgeniy Druzhinin, Georgy Zaytsev eta Ilya Karpov ikertzaileek mota hauetako hainbat ahultasun antzeman dituzte: bufferrak gainezka egitea, informazioa agerian geratzea eta Phoenix Contact-en FL switch kudeatuei eragiten dieten komandoen exekuzioa. Erasotzaile batek zerbitzuaren ukapen bat lor lezake, komandoen injekzioa burutu edo informazio sentikorra ikusi, ahultasun horiek baliatuta.

Konponbidea:

Firmwarea 1.34 bertsiora edo goragoko batera eguneratzea gomendatzen da, ahultasun horiek konpontzeko.

Phoenix Contact enpresak, gainera, kaltetutako bertsioetan switchen Web eragilea desgaitzeko gomendioa eman du, aldi baterako neurri moduan.

Xehetasuna:

- Kaltetutako gailuetara konfigurazio fitxategiak edo firmware eguneratzeko baimenak bidaltzeko aukera duen erasotzaile batek CGI ?config_transfer.cgi? eta ?software_update.cgi? fitxategien eskaera konprobaketaren ahultasun bat baliatu lezake sistema eragilearen komandoak exekutatu eta sareko zerbitzuaren ukapen bat lortzeko. Larritasun kritikoko ahultasun horretarako CVE-2018-10730 kodea erreserbatu da.
- Erasotzaile batek bereziki diseinatutako ?cookie? bat bidal lezake bufferrak gainezka egitea eragiteko. Horrela, sistema eragileko fitxategietara baimenik gabe sar liteke eta fitxategiak sartu, urrutitik kodea exekutatu eta gailuaren segurtasun egoera konprometituta geratzeko. Larritasun kritikoko ahultasun horretarako CVE-2018-107228 kodea erreserbatu da.
- Erasotzaile batek bereziki diseinatutako GET eskaerak bidal litzake, cookie, a ?menú_pxc.cgi? o ?index.cgi? eremua baliatuz, bufferrak gainezka egitea eraginez, eta Web edo Telnet zerbitzuak desgaituz zerbitzua ukatzeko, edo kodea urrutitik exekutatzeko. Larritasun kritikoko ahultasun horretarako CVE-2018-10731 kodea erreserbatu da.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna

Fitxategi lokalen barneratzea ABBren Ellipse v8-n

Argitalpen data: 2018/05/18

Garrantzia: Handia

Kaltetutako baliabideak:

- Ellipse, 8.3tik 8.9 bitarteko bertsioak

Azalpena:

ABBk Ellipse aplikazioari eragiten dion ahultasun bati buruzko informazioa jaso du. RSS funtzio batean dagoen ahultasuna da, eta hori baliatuz erasotzaile batek fitxategi lokalen sisteman gordetako fitxategietara sarbidea lor lezake urrunetik.

Konponbidea:

ABBk ahultasun hau konpontzen duten eguneraketa batzuk garatu ditu eta Ellipse aplikazioaren kaltetutako bertsioak lehenbailehen eguneratzea aholkatzen du, segurtasun arazoak konpontzen dituen bertsio berriago batera.

Xehetasuna:

- Ellipse aplikazioaren kaltetutako bertsioek dituzten funtzionaltasun batzuek erabiltzaileei ahalbidetzen diete RSS iturriak konfiguratzen URL baliozkoak baliatuz. Fitxategien sistema lokalera daraman URL bat baliatuz, erasotzaile batek datu konfidentzialak eskura litzake. Ekintza honen zergatia da aplikazioaren erabiltzaileen aldetik sarrera datuen baliozkotze okerra.

Etiketak: Eguneraketa, Nabigatzailea, Ahultasuna

Datu sentikorren zifratzerik eza Medtronic-en N'Vision Clinician Programmer-en

Argitalpen data: 2018/05/18

Garrantzia: Txikia

Kaltetutako baliabideak:

- 8840 N'Vision Clinician Programmer, bertsio guztiak.
- 8870 N'Vision removable Application Card, bertsio guztiak.

Azalpena:

Whitescope LLCren Billy Rios-ek ahultasun honen berri eman dio NCCICri. Ahultasunak datu sentikorrak eskuratzea ahalbidetu lezake.

Konponbidea:

Medtronicek ez du garatu ahultasun hau konpontzeko inolako eguneraketarik, baina erabiltzaileei aholkatzen die segurtasun neurri osagarriak hartzea ahultasun hau baliatzeko arriskua gutxitzearren. Klinikek eta ospitaleek ondokoa egin beharko lukete:

- 8870 aplikazio txartelak fisikoki zorrotz kontrolatzea.
- Soilik erabiltzea legitimoki eskuratutako 8870 txartelak eta ez hirugarren batzuek emandakoak. Izan ere, Medtronicek firmwarearen eta sistemaren eguneraketak eskaintzen ditu 8870 txartel berriak erabiliz.
- 8840 programatzaileak eta 8870 txartelak Medtronic-enak dira eta Medtronic-i itzuli behar zaizkio erabiltzeari utzitakoan. Hori ez bada posible, modu seguruan bota behar dira.

Xehetasuna:

Kaltetutako produktuan gordetako datuak ez daude zifratuta. Sarbide fisikoa lukeen erasotzaile batek ondoko informazioa eskura lezake:

- PII - Identifikaziorako informazio pertsonala. Norbanako baten zalantzarik gabeko identifikazioa ahalbidetzen duen datu pertsonalen konbinazioa.
- PHI - Osasun arloko informazio pertsonala. PIIren eta osasun arloarekin zerikusia duten datu osagarrien konbinazio bat.

Ahultasun horretarako CVE-2018-8849 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Sarrera parametroetan baliozkotze okerra General Electric-en produktuetan

Argitalpen data: 2018/05/18

Garrantzia: Handia

Kaltetutako baliabideak:

- PACSystems RX3i CPE305/310, 9.20 bertsioa eta lehenagokoak.
- RX3i CPE330, 9.21 bertsioa eta lehenagokoak.
- RX3i CPE 400, 9.30 bertsioa eta lehenagokoak.
- PACSystems RSTi-EP CPE 100, bertsio guztiak.
- PACSystems CPU320/CRU320 eta RXi, bertsio guztiak.

Azalpena:

Nozomi Networks-eko Younes Dragoni-k NCCICri eman dio ahultasun honen berri. Sarrera parametroetan baliozkotze okerraren erako ahultasuna da. Ahultasun hau urrunetik baliatuz gero, erasotzaile batek kaltetutako sistema berrabiaraz lezake edo gailuaren egoeran aldaketak eragin. Horrek kaltetutako gailuaren erabilezintasun egoera eragin lezake.

Konponbidea:

Ahultasun hori arintzen duen firmwarearen bertsio berri bat argitaratu du General Electricek.

- IC695CPE305 - https://digitalsupport.ge.com/communities/en_US/Download/IC695CPE305-PACSystems-RX3i-CPU-DN
- IC695CPE310 - https://digitalsupport.ge.com/communities/en_US/Download/IC695CPE310-PACSystems-RX3i-CPU-DN
- IC695CPE330 - https://digitalsupport.ge.com/communities/en_US/Download/IC695CPE330-PACSystems-RX3i-CPU-DN
- IC695CPE400 - https://digitalsupport.ge.com/communities/en_US/Download/IC695CPE400-PACSystems-RX3i-Rackless-CPU-with-Field-Agent
- CPE100 - https://digitalsupport.ge.com/communities/cc_login?startURL=/en_US/Download/EPSCPE100-RSTi-EP-CPU-Firmware
- CPU/CRU320 - General Electricek adierazi duenez, gailu modelo hau bere bizitza erabilgarriaren amaieran dago, eta horregatik modelo berriago batengatik aldatzea gomendatzen du.

Xehetasuna:

- Sarrera parametroen baliozkotze okerra. Ahultasun hau baliatuz erasotzaile batek kaltetutako gailuan erabilezintasun egoera eragin lezake, bereziki diseinatutako paketeekin eskaerak bidaliz. Ahultasun horretarako CVE-2018-8867 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Bufferraren gainezkatzea Delta Electronics-en Industrial Automation TPEditor-en

Argitalpen data: 2018/05/18

Garrantzia: Handia

Kaltetutako baliabideak:

- Delta Industrial Automation TPEditor, 1.89 eta lehenagoko bertsioak.

Azalpena:

ThePotato izenaz ezaguna den ikerlariak, Trend Micro-ren Zero Day Initiative-rekin (ZDI) lankidetzan, bufferraren gainezkatze erako ahultasuna aurkitu du Delta Electronics-en Industrial Automation TPEditor programazio softwarean. Erasotzaile batek bufferrak gainezka egitea eragin lezake, eta horrekin kodea urrutitik exekuta lezake.

Konponbidea:

Delta Electronicsek lanean dihardu bertsio berri bat prest izateko ahultasun hau gainditzearren. Bitartean, sarbideak mugatzea aholkatzen du, eta soilik fitxategi egiaztatuak erabiltzea.

Xehetasuna:

Industrial Automation TPEditor programak duen fitxategiak kudeatzeko modu okerrak bufferraren gainezkatzea eragin dezake. Sarbidea lukeen erasotzaile batek egoera hori balia lezake bereziki diseinatutako fitxategi baten bitartez, eta horrek kodea urrunetik exekutatzea ahalbidetuko lioke. Ahultasun horretarako CVE-2018-8871 kodea erreserbatu da.

Etiketak: 0day, Ahultasuna

Pasahitz barneratuak Yokogawa-ren STARDOM kontrolatzaileetan

Argitalpen data: 2018/05/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

STARDOM kontrolatzaileak:

- FCJ, R4.02 bertsioa edo lehenagokoak.
- FCN-100, R4.02 bertsioa edo lehenagokoak.
- FCN-RTU, R4.02 bertsioa edo lehenagokoak.
- FCN-500, R4.02 bertsioa edo lehenagokoak.

Azalpena:

Yokogawak STARDOM kontrolatzaileek daukaten pasahitz barneratuen ahultasun baten berri eman du. Erasotzaile batek sistemaren komandoak exekuta litzake.

Konponbidea:

Ahultasun hau konpontzeko Yokowagak R4.10 bertsiora edo berriago batera eguneratzea aholkatzen du.

Xehetasuna:

Kaltetutako produktuek barneratuta dauzkate erabiltzailea eta pasahitza. Arriskua dago barneratutako kontuarekin erasotzaile batek kontrolatzailean saioa hasi eta sistemaren komandoak exekuta ditzan.

Etiketak: Eguneraketa, Ahultasuna

Kredentzial barneratuak mySCADAren myPRO 7-n

Argitalpen data: 2018/05/22

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- myPRO 7

Azalpena:

Emre ÖVÜNÇ zibersegurtasun ikerlariak barneratutako kredentzialen ahultasun bat aurkitu du mySCADAren HMI/SCADA myPRO 7 softwarean. Erasotzaile batek kredentzial horiek balia litzake FTP zerbitzura konektatzeko eta fitxategiak igotzeko edo jaisteko.

Konponbidea:

Ez dago partxe edo eguneraketarik ahultasun hori konpontzeko. Une honetan dagoen konponbide bakarra 2121 atakarako trafikoa mugatzea da.

Xehetasuna:

myPROren azken bertsioak (v7) erabiltzailearen informazioa eta 2121 atakako ftp zerbitzariaren pasahitza fitxategi batean barneratuta dauzka. Erasotzaile batek kredentzial horiek balia litzake fitxategiak igo edo jaisteko myPRO softwarea exekutatzen duen zerbitzarian. Ahultasun horretarako CVE-2018-11311 identifikatzailea erreserbatu da.

Etiketak: Komunikazioak, Ahultasuna

Ekintza ez seguruen ohartarazpen gabezia Becton, Dickinson and Company-ren (BD) BD Kiestra eta InoqulA sistemetan

Argitalpen data: 2018/05/23

Garrantzia: Ertaina

Kaltetutako baliabideak:

Ahultasunek kaltetutako aplikazioak ondoko sistemek erabiltzen dituzte:

- BD Kiestra TLA
- BD Kiestra WCA
- BD InoqulA-ren lagin prozesatzailea

Ahultasunek kaltetutako aplikazioak honakoak dira:

- Database (DB) Manager, 3.0.1.0 bertsioa
- ReadA Overview, 1.1.0.2 eta lehenagoko bertsioak
- PerformA, 3.0.0.0 eta lehenagoko bertsioak

Azalpena:

BDk bi ahultasun aurkitu ditu, ekintza ez seguruen ohartarazpenak ez egitearen erakoak. BD Kiestra eta InoquIA sistemei eragiten diete. Erasotzaile batek datuak galtzea edo ezabatzea eragin lezake.

Konponbidea:

BDk 2018ko ekaina baino lehen izan nahi ditu prest beharrezkoak diren konponbideak.Konponbide horien bidez DB Manager, PerformA eta ReadA-n SQL funtzioak aktibatzeko funtzionaltasuna ezabatu ahal izango da. Hori egin bitartean, eta ahultasun horiekin lotutako arriskua gutxitzearren, BDk ondorengo kontrolak gomendatzen ditu:

- DB Manager:
  - BD Kiestra Laboratoryko langileek ez dituzte erabili behar funtzionaltasunari lotutako SQL funtzioak BD Kiestra hiru sistemetan: BD Kiestra TLA, BD Kiestra WCA eta BD InoqulA lagin prozesatzailearena. Oraingo programak esportatu-inportatu funtzioaren bidez ez erabiltzea gomendatzen da, baizik eta programa berri bat konfiguratzea edo programaren txantiloi lehenetsiak erabiltzea.
  - Komeni da ziurtatzea langile baimendu eta kualifikatuek soilik izango dituztela DB Manager-en funtzio guztietarako sarbide kontrolerako eskubideak. DB Manager-en 'Erabiltzaileak' funtzioaren bidez konfigura daiteke hori.
- ReadA Overview: erabiltzaileei gomendatzen zaie, aplikazioa erabiltzen ez bada edo erabiltzea ohikoa ez bada, ReadA Overview-ra sartzeko 'Users' funtzioa 'none' moduan konfiguratzea erabiltzaile guztientzat. DB Manager-en 'Users' funtzioaren bidez konfigura daiteke hori. ReadA Overview erabiltzea beharrezkoa bada, erabiltzaileei gomendatzen zaie langile baimendu eta kualifikatuek soilik izatea sarbide kontrolerako eskubideak ReadA Overview-ren funtzio guztietara. DB Manager-en 'Users' funtzioaren bidez konfigura daiteke hori.
- PerformA: BD Kiestra sistemetara baimenik gabeko sarbidea modu eraginkorrean saihestea lortuko duten segurtasun praktika onenak ezartzen diren bitartean, erabiltzaileei gomendatzen zaie BD Kiestrako zerbitzarietara sarbidea bermatzea horiek monitorizatu ahal izateko.

Xehetasuna:

DB Manager, PerformA eta ReadAri eragiten dien ahultasun bat baliatuz, sarbide altuekin baimendutako erabiltzaile batek BD Kiestra sisteman SQL komandoak erabili ahal izango lituzke, edo ondorioz datuen hondatzea eragin lezake. Ahultasun horietarako CVE-2018-10593 eta CVE-2018-10595 identifikatzaileak erreserbatu dira.

Etiketak: Ahultasuna

Hainbat ahultasun Schneider Electric-en PlantStruxure PES eta SoMachine Basic-en

Argitalpen data: 2018/05/24

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- PlantStruxure PES V4.3 SP1 eta lehenagoko bertsioak
- SoMachine Basic v1.6 SP1 eta lehenagoko bertsioak

Azalpena:

Applied-eko Gjoko Krstikj zibersegurtasun ikerlariak eta Schneider Electric-ek PlantStruxure PES lizentzia kudeatzailean erabiltzen den

Flexera FlexNet Publisher softwareari eta SoMachine Basic-i eragiten dieten hainbat ahultasun aurkitu dituzte. Erasotzaile batek ahultasun horietako batzuk balia litzake komandoak exekutatu ahal izateko, erabiltzaile legitimoak beste orrialde batzuetara birbidaltzeko edo zerbitzuaren ukapena eragiteko.

Konponbidea:

- Schneider Electric-ek lizentzia kudeatzailearen 2.1.0.0 bertsioa garatu du eta horrek PlantStruxure PESi eragiten dioten ahultasunak konpontzen ditu. Ondoko loturak eskura daiteke: https://www.pes.schneider-electric.com/software-downloads/software/895-floating-license-manager-v2-1-0-0?acm=9_47
- Schneider Electricek erabiltzaileen eskura jarri du SoMachine Basic-en ahultasuna konpontzeko eguneraketa. Lotura honetan eskura daiteke: https://www.schneider-electric.com/en/download/document/SoMachineBasicV1.6SP1/

Xehetasuna:

- Bufferrak gainezka egitea: OpenSSL 1.0.2h-k modu okerrean erabiltzen ditu biltegiratze mugen egiaztapenak eta hori baliatuz urruneko erasotzaile batek zerbitzuaren ukapena eragin lezake (osokoa gainezkatzea eta aplikazioa blokeatzea). Larritasun kritikoko ahultasun horretarako 2016-2177 identifikatzailea erabili da.
- Bufferrak gainezka egitea: FlexNet Publisher Licensing zerbitzua balia liteke memoriaren mugez kanpoko irakurketa eragiteko. Horren bitartez erasotzaile batek kode arbitrarioa exekuta lezake SYSTEM baimenekin. Larritasun altuko ahultasun horretarako CVE-2016-10395 identifikatzailea erabili da.
- Birbideratze irekia: Flexera FlexNet Publisher 11.14.1 eta lehenagoko bertsioetako lmadmin osagaia baliatuz erasotzaile batek erabiltzaileak webgune arbitrarioetara birbidera litzake eta zehaztu gabeko bektoreen bidez phising erasoak egin. Larritasun ertaineko ahultasun horretarako CVE-2017-5571 identifikatzailea erabili da.
- XML (XXE) Kanpo Entitatea: DTD parametroen entitateen teknika baliatuz, kaltetutako nodoan erasotzaile batek datu arbitrarioak hedatzea eta berreskuratzea lor lezake bandaz kanpoko erasoaren bidez (OOB). Ahultasuna sortzen da xml analizatzaileari ematen zaion informazioa normalizatzen ez denean proiektu/txantiloiaren xml fitxategia aztertutakoan. Larritasun altuko ahultasun horretarako CVE-2018-7783 identifikatzailea erabili da.

Etiketak: Eguneraketa, Schneider Electric, Ahultasuna

Hainbat ahultasun BeaconMedaes-en TotalAlert Scroll Medical Air Systems-en

Argitalpen data: 2018/05/25

Garrantzia: Handia

Kaltetutako baliabideak:

- TotalAlert Scroll Medical Air Systems, 4107600010.23 bertsioa edo lehenagokoa duen softwareduna.

Azalpena:

Maxim Rupp ikerlariak hainbat ahultasun aurkitu ditu BeaconMedaes-en TotalAlert Scroll Medical Air Systems izeneko osasun baliabideari eragiten diotenak. Erasotzaile batek gailuaren eta web aplikazioaren konfigurazioaren informazioa ikus eta alda lezake, nahiz eta ez lukeen sarbiderik izango erabiltzailearen osasun informaziora. BeaconMedaesek jakinarazi du arrakastaz egindako eraso batek ez liokeela eragingo aldez aurretik finkatutako funtzionamendu moduari.

Konponbidea:

BeaconMedaesek 4107600010.24 bertsioa garatu du, eta erabiltzaile guztiei aholkatzen die beren ekipoak azken bertsiora eguneratzea.

Xehetasuna:

- Kredentzialen babes okerra: Integratutako web zerbitzarira sareko sarbidea lukeen erasotzaile batek lehenetsitako kredentzialak edo erabiltzaile batenak berreskura litzake, modu ez seguruan gorde eta transmititu badira. Larritasun altuko ahultasun horretarako CVE-2018-7518 identifikatzailea erreserbatu da.
- Babesik gabe gordetako kredentzialak: Pasahitzak testu argian gordetzen dira, autentifikaziorik gabe eskura daitekeen fitxategi batean. Larritasun altuko ahultasun horretarako CVE-2018-7515 identifikatzailea erreserbatu da.
- Sarbide kontrol ezegokia: Erasotzaile batek web zerbitzarian URL jakin batera sar liteke eta aplikaziotik informazioa eskuratu autentifikatu gabe. Larritasun ertaineko ahultasun horretarako CVE-2018-7526 identifikatzailea erreserbatu da.

EtiketakEtiketak: Eguneraketa, Ahultasuna