2018ko Abenduaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Autentifikazio desegokia Bosch-en Access Easy Kontrolagailuetan

Argitalpen data: 2018/12/04

Garrantzia: Ertaina

Kaltetutako baliabideak:

- Access Easy kontrolagailua, 2.1 bertsioa

Azalpena:

Maxim Rupp ikertzaile independenteak autentifikazio desegokiko ahultasun bat aurkitu du Boschen Access Easy kontrolagailuetan. Hori baliatuz, erasotzaile batek gailuaren baliabideetara sarbidea lor lezake.

Konponbidea:

Firmwarearen 2.1.9.3 bertsiora eguneratzea

Xehetasuna:

- Access Easy gailuak gSOAP zerbitzua erabiltzen du datuak denbora errealean berreskuratzeko eta sentsorearen egoera bezeroen nabigatzaileetarako. Erasotzaile batek SOAPen azken URL konexioa ezagutuz gero, gailura sarbidea lor lezake erabiltzailearen baimenik gabe eta gailuaren interfazea erabili.

Etiketak: Eguneraketa, Ahultasuna

Cross-site Scripting erako ahultasuna SpiderControl-en SCADA Webserver-en

Argitalpen data: 2018/12/05

Garrantzia: Ertaina

Kaltetutako baliabideak:

- SCADA Webserver, 2.03.0001 baino lehenagoko bertsioak

Azalpena:

Ismail Bulbul ikertzaile independenteak *Reflected cross-site Scripting* (RXSS) erako ahultasun baten berri eman du, SpiderControl-en SCADA Webserver ekipoei eragiten diena.

Konponbidea:

- SCADA Webserver 2.03.0001 bertsiora eguneratzea

Xehetasuna:

- Islatutako guneen (ez iraunkorrak) arteko komandoen sekuentziak baliatuz, erasotzaile batek bereziki diseinatutako URL bat bidal lezake JavaScript edukiarekin, web aplikaziotik biktimaren nabigatzailean isla dadin. Ahultasun horretarako CVE-2018-18991 identifikatzailea erabili da.

Etiketak: Eguneraketa, Nabigatzailea, SCADA, Ahultasuna

Hainbat ahultasun Omron-en CX-One softwarean

Argitalpen data: 2018/12/05

Garrantzia: Ertaina

Kaltetutako baliabideak:

- CX-One, 4.42 bertsioa eta lehenagokoak, ondoko aplikazioak barne:
  - CX-Programmer, 9.66 bertsioa eta lehenagokoak.
  - CX-Server, 5.0.23 bertsioa eta lehenagokoak.

Azalpena:

Source Incite-ko Esteban Ruiz ikertzaileak, Trend Micro-ko Zero Day Initiative-rekin lankidetzan, bufferaren gainezkatze erako eta aurretiaz askatutako memoriaren erabilpen erako hainbat ahultasun aurkitu ditu Omron-en CX-One produktuetan. Ahultasun horiek arrakastaz baliatuz gero, erasotzaile batek kodea exekuta lezake aplikazioaren pribilegioekin.

Konponbidea:

Omronek ahultasun horiek konpontzen dituzten bertsio berriak argitaratu ditu:

- CX-Programmer, 9.70 bertsioa
- Modulu amankomuna, CX-Server barne, 5.0.24 bertsioa

Xehetasuna:

- Erasotzaile batek bereziki manipulatutako proiektu fitxategi bat erabil lezake bufferraren tamaina gainezkatzeko eta kodea exekutatu ahal izateko aplikazioaren pribilegioekin, horrela pilan oinarritutako bufferraren gainezkatzea eraginez (*stack based buffer overflow*). Ahultasun horretarako CVE-2018-18993 identifikatzailea erabili da.
- Bereziki aldatutako fitxategi bat erabiliz, erasotzaile batek urrunetik kodea exekutatzea lor lezake aplikazioaren pribilegioekin, askatutako memoriarako erreferentzien egiaztapenean dagoen akats bat baliatuz. Ahultasun horretarako CVE-2018-18989 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Rockwell Automation-en Allen-Bradley PowerMonitor-en

Argitalpen data: 2018/12/05

Garrantzia: Handia

Kaltetutako baliabideak:

- PowerMonitor 1000

Azalpena:

Luca Chiou ikertzaileak hainbat ahultasun aurkitu ditu, sarbidearen kontrol desegokiaren eta cross-site scripting erakoak, Allen-Bradley-ren PowerMonitor 1000 produktuan. Erasotzaile batek erabiltzaile berriak sor litzake gailuan edo XSS kodea injektatu.

Konponbidea:

Ez dago konponbiderik ahultasun horietarako.

Xehetasuna:

- Sarbidearen kontrol desegokia baliatuz urruneko erasotzaile batek proxya erabil lezake gailuaren funtzioak gaitzeko. Horrela erabiltzaile berriak sor litezke. Ahultasun horretarako CVE-2018-19616 kodea erabili da.
- Erasotzaile batek XSS kodea injekta lezake erabiltzailearen kontuko parametro batean, datu basean gordeko litzatekeena.

Etiketak: 0day, Ahultasuna

Aski ez den murrizpena kanpoko XML entitatearen erreferentzietan GEren Proficy GDSn

Argitalpen data: 2018/12/07

Garrantzia: Handia

Kaltetutako baliabideak:

Cimplicity, 9.0 R2, 9.5 eta 10.0 bertsioak

Azalpena:

Kaspersky Lab-eko Vladimir Dashchenko ikertzaileak General Electric-en Proficy GDSri eragiten dion ahultasun baten berri eman du, kanpoko XML entitatearen erreferentzietan aski ez den murrizpen baten erakoa. Hori baliatuz erasotzaile batek OPC UA saio bat has lezake eta xede duen sistemako fitxategiren bat berreskuratu.

Konponbidea:

- GEk bere bezeroei aholkatzen die 2.1 bertsiora edo goragoko batera eguneratzea.

Xehetasuna:

- XXE (XML External Entity) erreferentzien murrizpen desegoki bat baliatuz eta XXE injekzioen bidez, Proficy zerbitzariaren barneko bide batera irits liteke, OPC UA saio bat hasi eta xede den sistemako fitxategiak berreskuratu. Ahultasun horretarako CVE-2018-15362 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Zifratze ahula Philips-en HealthSuite Health Android aplikazioan

Argitalpen data: 2018/12/07

Garrantzia: Txikia

Kaltetutako baliabideak:

- Aplicación Android HealthSuite Health, bertsio guztiak.

Azalpena:

Ikertzaile anonimo batek Philipsen HealthSuite Health Android aplikazioaren komunikazioetan dagoen zifratu eskasaren erako ahultasun baten berri eman du. Hori baliatuz, gailura sarbide fisikoa lukeen erasotzaile batek aplikazioaren konfidentzialtasuna eta integritatea arriskuan jar litzake.

Konponbidea:

- Ahultasun hori konponduko duen Android aplikazioaren bertsio berria 2019ko lehen hiruhilekoan egongo da eskuragarri.
- Ahultasunaren aurreko arintze behin-behineko modura, Philipsek ondoko jokabideak gomendatzen ditu:
  - Root-a edo jail-break bat egin zaien gailu mugikorretan konfigurazio batzuk alda daitezke sistemak berez baimentzen dituenetatik harago. Horregatik, kaltetua izan den honetan bezala, garatutako aplikazioetan ezartzen diren murrizpenek agian ez dute izango nahi den ondorioa. Root edo jail-break bat eginez murrizpenak gainditzeak aplikazioen errendimenduan eragin dezake, gailuaren segurtasuna ahuldu eta, kasu honetan, Android sisteman dauden erabiltzaileak arrisku gehigarrietan jarri.

Xehetasuna:

- Kaltetutako softwareak erabiltzen duen zifratua ahultzat jotzen da. Gailura sarbide fisikoa lukeen erasotzaile batek produktuaren konfidentzialtasuna eta integritatea arriskuan jar litzake. Ahultasun horretarako CVE-2018-19001 identifikatzailea erabili da.

Etiketak: Ahultasuna

Hainbat ahultasun Schneider Electric-en Eurotherm GUIcon-en

Argitalpen data: 2018/12/07

Garrantzia: Handia

Kaltetutako baliabideak:

- Eurotherm GUIcon Versión 2.0 Gold Build 683.0

Azalpena:

9SG Security Team-eko mdm eta rgod ikertzaileek Schneider Electric-i datu bateraezinen moten erabilpen erako eta bufferraren gainezkatze erako hainbat ahultasunen berri eman diote. Horiek baliatuz erasotzaile batek kodea urrunetik exekuta lezake.

Konponbidea:

- GUIcon-en Version 2.0 Software Package (Gold Build 683.003) bertsiora eguneratu

Xehetasuna:

- GD1 fitxategiak prozesatzean pcwin.dll-n datu bateraezinen moten erabilpen erako ahultasun bat baliatuz, erasotzaile batek kodea exekuta lezake urrunetik. Ahultasun horretarako CVE-2018-7813 identifikatzailea erabili da.
- GD1 fitxategiak prozesatzean, pilan oinarritutako bufferraren gainezkatzearen erako ahultasun bat baliatuz erasotzaile batek urrunetik kodea exekuta lezake. Ahultasun horretarako CVE-2018-7814 identifikatzailea erabili da.
- GD1 fitxategiak prozesatzean c3core.dll-n datu bateraezinen moten erabilpen erako ahultasun bat baliatuz, erasotzaile batek kodea exekuta lezake urrunetik. Ahultasun horretarako CVE-2018-7815 identifikatzailea erabili da.

Etiketak: Schneider Electric, Ahultasuna

Ahultasuna Eaton-en xComfort-en

Argitalpen data: 2018/12/10

Garrantzia: Handia

Kaltetutako baliabideak:

- Adimendun etxeen xComfort kontrolatzailea (*Smart Home Controller*, SHC), SHC-7.5-2.3.2 bertsioa eta lehenagokoak.

Azalpena:

Eatonek adimendun etxeen xComfort kontrolatzaileari (SHC) eragiten dion ahultasun baten berri eman du.

Konponbidea:

Eatonek *firmwarearen* SHC-7.5-2.3.3 bertsioa argitaratu du, ahultasuna konpontzen duena.

Xehetasuna:

- Oraingoz ez dago informazio gehiago.

Etiketak: Eguneraketa, Pribatutasuna, Ahultasuna

Hainbat ahultasun Siemensen produktuetan

Argitalpen data: 2018/12/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SINUMERIK 808D V4.7, bertsio guztiak.
- SINUMERIK 808D V4.8, bertsio guztiak.
- SINUMERIK 828D V4.7, V4.7 SP6 HF1 baino lehenagoko bertsio guztiak.
- SINUMERIK 840D sl V4.7, V4.7 SP6 HF5 baino lehenagoko bertsio guztiak.
- SINUMERIK 840D sl V4.8, V4.8 SP3 baino lehenagoko bertsio guztiak.
- SINAMICS PERFECT HARMONY GH180, A30 eta MLFB 6SR325 aukerak dituzten driver hauekin: MLFB 6SR32, MLFB 6SR52, MLFB 6SR42.
- TIM 1531 IRC, V2.0 baino lehenagoko bertsio guztiak.

Azalpena:

Kaspersky Lab eta McAfee Corporation-eko Anton Kalinin, Danila Parnishchev, Dmitry Sklyar, Gleb Gritsai, Kirill Nesterov, Radu Motspan eta Sergey Sidorov ikertzaileek Siemensekin koordinatu dute hainbat ahultasunen tratamendua: fitxategien baimenetan kontrol gabeziaren bidalketa, pribilegioen eskalatzea, bufferraren gainezkatzea, autentifikazio desegokia eta kontrol falta ioctl deietan. Horiek baliatuz erasotzaile batek hainbat kalte eragin litzake: zerbitzuaren ukapena, kode gaiztoa exekutatzea, pribilegioen eskalatzeak edo kaltetutako gailuen funtzionamendu okerra.

Konponbidea:

- CVE-2018-11457, CVE-2018-11458, CVE-2018-11459, CVE-2018-11460, CVE-2018-11461, CVE-2018-11462, CVE-2018-11463, CVE-2018-11464, CVE-2018-11465 eta CVE-2018-11466 ahultasunen kasuan, Siemensek ondokoa gomendatzen du:
  - Suebakiak X130 ataketarako dituen lehenetsitako konfigurazioak berrikustea eta berrezartzea (4842/tcp eta 5900/tcp atakak blokeatuta).
  - Kaltetutako produktuetarako sarbidea murriztea baimendutako pertsonalari soilik ahalik eta baimen gutxienekin.
  - Gelaxken babes kontzeptua aplikatzea.
  - VPN erabiltzea gelaxken artean sareko komunikazioak babesteko.
  - Defentsa sakonaren kontzeptua aplikatzea.
- CVE-2018-6690:
  - Diskorako sarbide lokala babestea.
  - Biltegiratzeko erabiltzen diren USB gailuak zurian eta malwaretik libre daudela ziurtatzea diskora konektatu baino lehen.
  - Gelaxken babes kontzeptua aplikatzea eta sakoneko defentsa inplementatzea.
- CVE-2018-13816:
  - 102/tcp atakarako sarbidea konfiantzako helbideetara soilik murriztea.
  - V2.0 firmwarearen bertsiora eguneratzea (eta ingeniaritzako TIM estazioa berrabiatzea).
- Informazio gehiago izateko ondoko loturak irakur daitezke:
  - https://www.siemens.com/cert/operational-guidelines-industrial-security.
  - https://www.siemens.com/industrialsecurity.

Xehetasuna:

Asmo txarreko erabiltzaile batek era ezberdinetako ahultasunen bat balia lezake:

- Bereziki diseinatutako paketeen bidalketa.
- Fitxategien baimenetan kontrol falta.
- CRAMFS fitxategien baimenetan kontrol falta.
- Pribilegioen eskalatzea.
- Bereziki diseinatutako paketeen bidalketa.
- Bufferraren gainezkatzea.
- Zerbitzuaren ukapena VNC zerbitzarian.
- Kontrol falta ioctl deietan.
- Bereziki diseinatutako paketeen bidalketa.
- Kodearen exekuzioa.
- Autentifikazio desegokia.

Ahultasun horietarako honako identifikatzaileak erreserbatu dira: CVE-2018-11457, CVE-2018-11458, CVE-2018-11459, CVE-2018-11460, CVE-2018-11461, CVE-2018-11462, CVE-2018-11463, CVE-2018-11464, CVE-2018-11465, CVE-2018-11466 eta CVE-2018-13816. Era berean, CVE-2018-11490 identifikatzailea esleitu da.

Etiketak: Eguneraketa, Siemens, Ahultasuna

Cross-site scripting erako ahultasuna OSIsoft-en PI Vision-en

Argitalpen data: 2018/12/12

Garrantzia: Ertaina

Kaltetutako baliabideak:

- PI Vision 2017
- PI Vision 2017 R2

Azalpena:

OSIsoft-ek cross-site scripting erako ahultasun bat aurkitu du, bere PI Vision produktuei eragiten diena. Hori baliatuz urruneko erasotzaile batek webguneko eta PI Vision aplikazioko atributu ezberdinak alda litzake.

Konponbidea:

- Ahultasuna konpontzeko OSIsoft-ek PI Vision 2017 R2 SP1 bertsiora eguneratzea gomendatzen du.

Xehetasuna:

- Kaltetutako produktuak JavaScript kodea erabiltzen du AF elementu eta atributuetan. Urruneko erasotzaile batek biktimaren nabigatzailean PI Visionen webguneko edukia eta PI Vision aplikazioarekin zerikusia duten datuak irakurri eta alda litzake. Horretarako AFren erabiltzaile baimendu batek AFren elementu eta atributuetan JavaScript gordetzeko trebetasuna izatea beharrezkoa da.

Etiketak: Eguneraketa, Ahultasuna

Bufferraren gainezkatzea Bosch-en IP kameretan

Argitalpen data: 2018/12/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Common Product Platform 7.3 (CPP7.3)
  - AUTODOME IP 4000i, 5000i, starlight 5000i (IR) eta starlight 7000i
  - DINION IP bullet 4000i, 5000i eta 6000i
  - FLEXIDOME IP 4000i eta 5000i
  - MIC IP starlight 7000i eta fusion 9000i
- CPP7:
  - DINION IP starlight 6000 eta 7000
  - DINION IP thermal 8000
  - FLEXIDOME IP starlight 6000 eta 7000
- CPP6:
  - DINION IP starlight 8000 12MP eta ultra 8000 12MP
  - FLEXIDOME IP panoramic 6000 12MP 180, 360, 180 IVA eta 360 IVA
  - FLEXIDOME IP panoramic 7000 12MP 180, 360, 180 IVA eta 360 IVA
  - AVIOTEC IP starlight 8000
- CPP4:
  - AUTODOME IP 4000 HD, 5000 HD, 5000 IR eta 7000 seriea
  - DINION HD 1080p, 1080p HDR, 720p
  - DINION imager 9000 HD
  - DINION IP bullet 4000, 4000 HD, 5000, 5000 HD, 5000 MP eta starlight 7000 HD
  - EXTEGRA IP dynamic 9000 eta starlight 9000
  - FLEXIDOME corner 9000 MP
  - FLEXIDOME HD 1080p, 1080p HDR eta 720p
  - FLEXIDOME IP panoramic 5000
  - FLEXIDOME IP indoor 5000 HD, 5000 MP, 4000 HD, 4000 IR,
  - FLEXIDOME IP outdoor 4000 HD, 4000 IR, 5000 HD, 5000 MP
  - FLEXIDOME IP micro 5000 HD, 5000 MP, 2000 HD eta 2000 IP
  - IP bullet 4000 HD eta 5000 HD
  - IP micro 2000 eta 2000 HD
  - MIC IP dynamic 7000 eta starlight 7000
  - TINYON IP 2000 family
  - Vandal-proof FLEXIDOME HD 1080p, 1080p HDR eta 720p

Azalpena:

- Ikertzaile independente batek bufferraren gainezkatze erako ahultasun bat aurkitu du Boschen IP kameretan. Hori baliatuz, erasotzaile batek urruneko kodea exekuta lezake kaltetutako gailuetan.

Konponbidea:

- Boschek gailuen firmwarea ondoko eguneraketetara eguneratzea gomendatzen du:
  - CPP guztien kasuan, ahultasun hori konpontzen duten firmwarearen bertsioak 6.51.0028, 6.50.0133 eta 6.44.0027 dira
- Erabilitako BVMSen (Bosch Video Management System) bertsioaren arabera, Boschek bertsio jakin bat ere aholkatzen du:
  - BVMS 7.0, 7.5, eta 8.0: 6.44.0027 bertsioa CPP guztietarako
  - BVMS 9.0: 6.51.0028 bertsioa CPP guztietarako

Xehetasuna:

- Urruneko erasotzaile batek bufferrak gainezka egitea eragin lezake. Horrekin kodea exekuta lezake, erabiltzaile eta pasahitzetara sarbidea lortu, aukerak aktibatu edo kaltetutako gailua blokeatu. Ahultasun horretarako CVE-2018-19036 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Sistema eragileko komandoen injekzioa Geutebrück GmbHren IP E2 kameretan

Argitalpen data: 2018/12/14

Garrantzia: Handia

Kaltetutako baliabideak:

- E2 serieko kamerak, 1.12.0.25 baino lehenagoko bertsioak

Azalpena:

- RandoriSec-eko Davy Douhine ikertzaileak sistema eragileko komandoen injekzio erako ahultasun bat aurkitu du Geutebrück GmbH-en E2 serieko IP kameretan. Hori baliatuz urruneko erasotzaile batek komandoak exekuta litzake "root" erabiltzaile modura.

Konponbidea:

- Geutebrück GmbHek firmwarearen 1.12.0.25 bertsioa argitaratu du

Xehetasuna:

- Kameraren konfigurazio paneleko DDNSren konfigurazioa baliatuz, urruneko erasotzaile batek komandoak exekuta litzake "root" erabiltzaile modura. Ahultasun horretarako CVE-2018-19007 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Datu sentikorren zifratze falta Medtronic-en CareLink eta Encore produktuetan

Argitalpen data: 2018/12/14

Garrantzia: Ertaina

Kaltetutako baliabideak:

- CareLink 9790 Programmer, bertsio guztiak.
- CareLink 2090 Programmer, bertsio guztiak.
- 29901 Encore Programmer, bertsio guztiak.

Azalpena:

Whitescope LLCko Billy Rios eta Jonathan Butts ikertzaileek datu sentikorren zifratze faltaren erako ahultasun bat aurkitu dute. Datu horiek osasun informazio babestua edo informazio pertsonal identifikagarria izan lezakete, eta ahultasuna baliatuz gailura sarbide fisikoa lukeen erasotzaile batek informazio hori irakur lezake.

Konponbidea:

- CareLink 9790 Programmer gailua zaharkitua dago, eta Medtronic-ek gomendatzen du gehiago ez erabiltzea. Gainera, CareLink 2090 Programmer eta 29901 Encore Programmer-en kasuan konpainiak aholkatzen du osasun informazioa eta informazio pertsonala ahalik eta denborarik laburrenean gordetzea gailu horietan. Era berean, segurtasun buletin bat argitaratu du ohartarazpen hau dela eta.

Xehetasuna:

- Urruneko erasotzaile batek datu sentikorren zifratze falta balia lezake gailu ezberdinetan gordeta dagoen osasun informazioa eta informazio pertsonala eskuratzeko. Ahultasun horretarako CVE-2018-18984 identifikatzailea erreserbatu da.

Etiketak: Azpiegitura kritikoak, Ahultasuna

Bide jauzia GEren Mark VIe-n

Argitalpen data: 2018/12/14

Garrantzia: Handia

Kaltetutako baliabideak:

- Mark VIe, 03.03.28Ctik 05.02.04Cra bitarteko bertsioak
- EX2100e, EX2100e_Reg eta LS2100e, v04.09.00C baino lehenagoko bertsioak

Azalpena:

Biznet Bilisim-eko Can Demirel ikertzaileak bide jauziaren erako ahultasun baten berri eman du, GEren DCS Mark Vie gailuei eragiten diena. Hori baliatuz, erasotzaile batek sistemako datuetara sarbidea lor lezake eta ondorioz baita pribilegioen eskalatzea eta kontrolatzailera baimenik gabeko sarbidea ere.

Konponbidea:

GEk ahultasun hori ControlST softwarearen oraingo bertsioarekin konpondu du. Erabiltzaile erregistratuek webgune honetan eskuratu dezakete: GE Power ServiceNow

Xehetasuna:

- Erasotzaile batek isilpeko informaziora sarbidea lor lezake bide jauziaren murrizpen erako akats bat baliatuz. Ahultasun horretarako CVE-2018-19003 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun ABBren GATE gailuetan

Argitalpen data: 2018/12/17

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- GATE-E2, bertsio guztiak.
- GATE-E1, bertsio guztiak.

Azalpena:

Applied Risk-eko Nelson Berg ikertzaileak *Cross-Site Scripting* (XSS) erako eta autentifikaziorako laguntzaren gabezia erako bi ahultasunen berri eman du, ABBren GATE gailuei eragiten dietenak. Erasotzaile batek gailuak egoera eskuraezinean utz litzake edo kodea injektatu.

Konponbidea:

Kaltetutako produktuak bere bizitza erabilgarriaren amaieran aurkitzen dira eta horregatik ABBk ez ditu argitaratuko ahultasun horiek konpontzeko firmware bertsio berriak.

Nolanahi ere, ABBk erabiltzaile guztiei emailez helarazi dizkie gailu horiek modu seguruan konfiguratzeko argibideak.

Gainera, ABBk hainbat gomendio egin ditu: baimenik gabeko langileek sarbide zuzenik izan ez dezaten gailuak babestea, Interneterako konexio zuzenik ez izatea, ekipo hauek beste batzuetatik babestea suebakiek kontrolatutako sareetan, eta ahalik eta ataka gutxien agerian uztea.

Xehetasuna:

- Erasotzaile batek *Cross-Site Scripting* bat egin lezake eta gailuak egoera eskuraezinean utzi gailuaren konfigurazioa aldatuz edo produktua modu iraunkorrean berrabiaraziz. Ahultasun horretarako CVE-2018-18997 identifikatzailea erreserbatu da.
- Autentifikazioaren uneko laguntza gabezia batek eraginda, urruneko erasotzaile batek *scriptak* injekta litzake bezeroaren aldean produktuaren webgunean. Horrela produktuaren web interfazera konektatuta dauden erabiltzaileen nabigatzailea arriskuan jar liteke. Ahultasun horretarako CVE-2018-18995 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna

Ahultasuna Eaton-en XP503-n

Argitalpen data: 2018/12/17

Garrantzia: Ertaina

Kaltetutako baliabideak:

- XP503 Visual Designer.
- XP503 Galileo.

Azalpena:

Eaton-ek Panel PC XP503ri eragiten dion ahultasun bat aurkitu du, Windows Embedded Standard 7ren erabilpenak eraginda.

Konponbidea:

Oraindik ez da konponbiderik argitaratu ahultasun honetarako.

- Eatonek XP503 gailuetarako bertsio berri bat programatu du 2019ko lehen hiruhilekorako.

Xehetasuna:

- Oraingoz ez dago informazio gehiago.

Etiketak: Ahultasuna

Sarreren baliozkotze okerra Advantech-en WebAccess/SCADAn

Argitalpen data: 2018/12/19

Garrantzia: Handia

Kaltetutako baliabideak:

- WebAccess/SCADA, Windows 2008 R2 SP1en instalatutako 8.32 bertsioa

Azalpena:

Tenable Network Security-ko Jacob Baines ikertzaileak sarreren baliozkotze okerraren erako ahultasun baten berri eman du, Advantech-en SCADA WebAccess/SCADA softwareari eragiten diona.

Konponbidea:

- Ahultasun hori konpontzeko Advantech-ek 8.3.4 eguneraketa argitaratu du.

Xehetasuna:

· Sarreren baliozkotze okerra baliatuz, urruneko erasotzaile batek bufferraren pilaren gainezkatzea eragin lezake. Ahultasun horretarako CVE-2018-18999 kodea erreserbatu da.

Etiketak: Eguneraketa, SCADA, Ahultasuna

Hainbat ahultasun 3S-Smart Software Solutions GmbHren CODESYS produktuetan

Argitalpen data: 2018/12/19

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- BeagleBone, emPC-A/iMX6, IOT2000, Linux, PFC100, PFC200 eta Raspberry Pi-rako CODESYS Control.
- Beckhoff CXerako CODESYS Control RTE V3 eta RTE V3.
- CODESYS Control Win V3 (CODESYSen konfigurazioaren zati bat ere bai).
- CODESYS Control V3 Runtime System Toolkit.
- CODESYS V3 Simulation Runtime (CODESYS Development System-en zati bat).
- CODESYS V3 Embedded Target Visu Toolkit.
- CODESYS V3 Remote Target Visu Toolkit.
- CODESYS V3 Safety SIL2.
- CODESYS V3 Development System.
- CODESYS Gateway V3.
- CODESYS HMI V3.
- CODESYS OPC Server V3.
- CODESYS PLCHandler SDK.

3S-Smart Software Solutions GmbH-k jakinarazi du CVE-2018-10612 kodeaz identifikatutako ahultasunak 3.5.14.0 bertsioa baino lehenagoko *CmpSecureChannel* edo *CmpUserMgr* osagaiak dituzten CODESYS Control V3 produktuen aldaera guztiei eragiten diela, zeinahi delarik haien CPU mota edo sistema eragilea.

Azalpena:

Kaspersky Lab-eko Alexander Nochvay eta Yury Serdyuk ikertzaileek 3S-Smart Software Solutions GmbHren CODESYS V3 eta CODESYS control V3 produktuei eragiten dieten hainbat eratako ahultasunen berri eman dute: aski ausazkoak ez diren balioen erabilpena, komunikazio kanalaren murrizpen desegokia eta sarbideen kontrol desegokia. Urruneko erasotzaile batek pakete gaiztoen jatorria ezkuta lezake, ausazko balioek duten ahultasun bat baliatu eta horrela datuen konfidentzialtasuna eta integritatea kaltetu, edo gailura baimenik gabeko sarbidea lor lezake eta informazio sentikorra zabaldu, erabiltzailearen kredentzialak barne.

Konponbidea:

- 3-S Smart Software Solutions GmbHk gomendatzen du 3.5.14.0 edo goragoko bertsiora eguneratzea, bere deskargen zentrotik. Gainera, CODESYSek online erabiltzaileen kudeaketarako eta komunikazioak zifratzeko duen kontrola aktibatzea ere gomendatzen du.

Xehetasuna:

- Aski ausazkoak ez diren balioen erabilpenak gailuan gordetzen diren datuen konfidentzialtasunari eta integritateari eragiten die. Ahultasun horretarako CVE-2018-20025 identifikatzailea erreserbatu da.
- Komunikazio kanalaren murrizpen desegokia baliatuz komunikazioan paketeen jatorria faltsutu liteke. Ahultasun horretarako CVE-2018-20026 identifikatzailea erreserbatu da.
- Erabiltzaileen sarbidearen kudeaketa desegokia dela-eta lehenespenez komunikazioaren zifratua desgaituta dagoela baliatuz, erasotzaile batek gailura eta informazio sentikorrera sarbidea lor lezake, erabiltzaileen kredentzialak barne. Ahultasun horretarako CVE-2018-10612 identifikatzailea erreserbatu da.
- Informazioaren sentikorraren agerpena.
- Zerbitzuaren ukapena.
- Zerbitzuaren urruneko ukapena.

Etiketak: Komunikazioak, Ahultasuna

URLren birbideratze erako ahultasuna Schneider Electric-en Power Monitoring Expert-en

Argitalpen data: 2018/12/20

Garrantzia: Handia

Kaltetutako baliabideak:

- EcoStruxure™ Power Monitoring Expert (PME), 8.2 (edizio guztiak) eta 9.0 bertsioak
- EcoStruxure™ Energy Expert (lehen Power Manager deitua), 1.3 eta 2.0 bertsioak
- EcoStruxure™ Power SCADA Operation (PSO) Advanced Reports eta Dashboards Module, 8.2 eta 9.0 bertsioak

Azalpena:

Business Integration Partners S.p.A-ko Donato Onofri ikertzaileak URLren birbideratze erako ahultasun baten berri eman du. Hori baliatuz urruneko erasotzaile batek *phishing* eraso bat eragin lezake, webgune gaizto batera birbideratuz.

Konponbidea:

- PME v8.2, Energy Expert v1.3 eta PSO v8.2 Advance Reports eta Dashboard Module-ren kasuan, deskargatu PME 8.2 CU3.
- PME v9.0, Energy Expert v2.0 eta PSO v9.0 Advance Reports eta Dashboard Module-ren kasuan, deskargatu CU1 18328.01.

Xehetasuna:

- Urruneko erasotzaile batek *phishing* eraso bat eragin lezake, erabiltzailea webgune gaizto batera birbideratuz. Ahultasun horretarako CVE-2018-7797 identifikatzailea erabili da.

Etiketak: Eguneraketa, Schneider Electric, Ahultasuna

Sarbidearen baliozkotze okerra Horner Automation-en Cscape-n

Argitalpen data: 2018/12/21

Garrantzia: Ertaina

Kaltetutako baliabideak:

- Cscape, 9.80.75.3 SP3 bertsioa eta lehenagokoak.

Azalpena:

9SG Security Team-eko rgod eta mdm ikertzaileek, Trend Microko Zero Day Initiativerekin lankidetzan, NCCICrako sarbidearen baliozkotze okerraren erako ahultasun baten berri eman dute.

Konponbidea:

- Ahultasuna konpontzeko Horner Automationek eskuragarri dagoen Cscaperen azken bertsiora eguneratzea gomendatzen du (9.80 SP4 bertsioa). Ondoko loturetan deskarga daiteke Amerikatik eta munduaren gainerako eskualdeetatik.

Xehetasuna:

- Erasotzaile batek bereziki diseinatutako POC fitxategi bat sor lezake Cscaperen softwareak prozesatua izateko, horrek ez baitu modurik fitxategi horiek baliozkotzeko erabiltzaile batek txertatzen dituenean. Hori baliatuz erasotzaileak informazio konfidentzialera sarbidea lor lezake eta urrunetik kode arbitrarioa exekutatu. Ahultasun horretarako CVE-2018-19005 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Bufferraren gainezkatzea Rockwell Automation-en FactoryTalk Services Platform-en

Argitalpen data: 2018/12/21

Garrantzia: Handia

Kaltetutako baliabideak:

· FactoryTalk Services Platform, 2.90 eta lehenagoko bertsioak.

Azalpena:

- Andrey Zhukov ikertzaileak bufferraren gainezkatze erako ahultasun baten berri eman du.

Konponbidea:

- Rockwellek bere deskargen zentroan eskuragarri dagoen azken bertsiora eguneratzea gomendatzen du.

Xehetasuna:

- Autentifikaziorik gabeko urruneko erasotzaile batek bereziki diseinatutako pakete ugari bidal litzake zerbitzu ataketara. Horrela memoriaren kontsumoa eragin lezake, eta ondorioz, kaltetutako zertzuetan zerbitzuaren ukapen egoera osoa edo partziala gerta liteke. Ahultasun horretarako CVE-2018-18981 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Zerbitzuaren ukapena Yokogawa-ren Vnet/IP Open Communication kontrolatzailean

Argitalpen data: 2018/12/21

Garrantzia: Handia

Kaltetutako baliabideak:

- CENTUM
  - CS 3000 eta CS 3000 Entry Class, R3.05.00tik R3.09.50era bitarteko bertsioak
  - VP eta VP Entry Class, R4.01.00tik R6.03.10era bitarteko bertsioak
- Exaopc, R3.10.00tik R3.75.00ra bitarteko bertsioak
- PRM, R2.06.00tik R3.31.00ra bitarteko bertsioak
- ProSafe-RS, R1.02.00tik R4.02.00ra bitarteko bertsioak
- FAST/TOOLS, R9.02.00tik R10.02.00ra bitarteko bertsioak
- B/M9000 VP, R6.03.01etik R8.01.90era bitarteko bertsioak

Azalpena:

Yokogawak zerbitzuaren ukapen erako ahultasun bat aurkitu du, bere Vnet/IP Open Communication kontrolatzaileari eragiten diona.

Konponbidea:

Ondoko produktuen kasuan ez dago inolako konponbiderik eskuragarri, Yokogawak adierazten duenez katalogoz kanpo baitaude dagoeneko eta horregatik bertsio berriago batera berritzea gomendatzen du:

- CENTUM CS 3000 eta CS 3000 Entry Class, R3.05.00tik R3.09.50era bitarteko bertsioak
- CENTUM VP eta VP Entry Class, R4 serieko bertsio guztiak
- Exaopc, R3.10.00tik R3.60.00ra bitarteko bertsioak
- PRM, R2.06.00tik R3.04.00ra bitarteko bertsioak
- ProSafe-RS, R1 eta R2 serieko bertsio guztiak

Ondoko produktuen kasuan, Yokogawak gomendatzen du Vnet/IP Open Communication kontrolatzailea R10.01.08 software bertsiora eguneratzea:

- CENTUM VP eta VP Entry Class, R5 serieko bertsio guztiak eta R6 seriean R6.03.10 bertsioa baino lehenagokoak
- Exaopc, R3.70.00tik R3.75.00ra bitarteko bertsioak (ahultasuna R3.76.00 bertsioan izan zen konpondua)
- PRM, R3.05.00tik R3.31.00ra bitarteko bertsioak (ahultasuna R4.01.00 bertsioan izan zen konpondua)
- ProSafe-RS, R3 serieko bertsio guztiak eta R4 seriean R4.02.00 baino lehenagoko bertsioak (ahultasuna R4.03.00 bertsioan izan zen konpondua)
- FAST/TOOLS, R9.02.00tik R9.05.00ra bitarteko bertsioak eta R10 seriean R10.02.00 baino lehenagoko bertsioak (ahultasuna R10.03.00bertsioan izan zen konpondua)
- B/M9000 VP, R6.03.01etik R8.01.90era bitarteko bertsioak.Gailu honi ahultasunak ez dio eragiten PC berean CENTUM VP instalatuta ez badago. Instalatutako CENTUM VP eguneratu beharra baldin badago, B/M9000 VP bertsio egoki batera eguneratu.

Xehetasuna:

- Zerbitzuaren ukapen erako ahultasun bat baliatuz, urruneko erasotzaile batek Vnet/IP Open Communication kontrolatzailearen komunikazio funtzioa geldi lezake.

Etiketak: Komunikazioak, Ahultasuna

Hainbat ahultasun Schneider Electric-en produktuetan

Argitalpen data: 2018/12/26

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- PowerSuite2ren bertsio guztiak (VW3A8104 & Patches)
- IIoT Monitor, 3.1.38 bertsioa
- Pro-Face GP-Pro EX, 4.08 eta lehenagoko bertsioak
- EVLink Parking, 3.2.0-12_v1 eta lehenagoko bertsioak
- Foxboro DCS eta Foxboro Evo-ren bertsio guztiak
- IA Series, Foxboro DCS Control Core Service 9.4 baino lehenagoko bertsioetan
- FoxView, 10.5 bertsioa

Azalpena:

Vahagn Vardanyan, Rgo (Zero Day Initiative), Yu Quiang (Venustech-eko ADLab) eta Vladimir Kononovich, Vyacheslav Moskvin eta Ilya Karpov (Positive Technologies) ikertzaileek, Schneider Electric-ekin elkarlanean, hainbat eratako ahultasunen berri eman dute: bufferraren gainezkatzea, murriztutako direktorioen kudeaketa desegokia, XMLren murrizketa okerra, fitxategien karga okerra, sarreraren baliozkotze okerra, SQL injekzioa, kredentzialen administrazio desegokia eta kodearen injekzioa. Horiek baliatuz erasotzaile batek kode gaiztoa exekuta lezake, gailuetara baimenik gabeko sarbidea lortu, pasahitzak baimenik gabe zabaldu edo aldatu, edo fitxategietara sarbidea lortu.

Konponbidea:

- PowerSuite 2k duen ahultasunerako Schneider-ek ondokoa gomendatzen du:
  - ATV11, ATV28, ATV38, ATV58, ATV58F edo Lexium05 modeloen kasuan: 27698 atakan urruneko edozein konexio eragotziko duen suebaki baten atzean konektatu ordenagailua.
  - Gainerako modeloen kasuan, *Remediation ataleko 2. puntuko* jarraibideak jarraitu.
- IIoT Monitor-ek dituen ahultasunetarako: Schneider Electric-en bezeroaren arreta zerbitzuarekin harremanetan jarri.
- Pro-Face GP-Pro EXek duen ahultasunerako: 4.08.200 bertsioa deskargatu
- EVLink Parking-ek dituen ahultasunetarako: *fix-a* deskargatu.
- FoxView HMI SCADAk duen ahultasunerako: Foxboro DCS Control Core Service 9.4 eta Foxview 10.5 bertsio berriagoetara eguneratu.

Xehetasuna:

Erasotzaile batek ahultasun horietakoren bat balia lezake gailuaren kontrola hartzeko edo bere funtzionamendu okerra eragiteko:

- Bufferraren gainezkatzea.
- Direktorio murriztuen kudeaketa desegokia.
- Fitxategien karga desegokia.
- XMLren murrizketa desegokia.
- Sarreren baliozkotze desegokia.
- Kodearen injekzioa.
- SQL injekzioa.
- Kredentzialen administrazio desegokia.

Ahultasun horietarako honako identifikatzaileak erabili dira: CVE-2018-7796, CVE-2018-7835, CVE-2018-7836, CVE-2018-7837, CVE-2018-7832, CVE-2018-7800, CVE-2018-7801, CVE-2018-7802 eta CVE-2018-7793.

Etiketak: Eguneraketa, Schneider Electric, Ahultasuna

Memoriaren hondatzea Schneider Electric-en Zelio Soft-en

Argitalpen data: 2018/12/28

Garrantzia: Handia

Kaltetutako baliabideak:

- Zelio Soft 2, 5.1 bertsioa eta lehenagokoak.

Azalpena:

9SG Security Team-eko mdm eta rgod ikertzaileek aurrez askatutako memoriaren erabilpen erako (*use after free*) ahultasun bat aurkitu dute. Hori baliatuz, erasotzaile batek kodea exekuta lezake urrunetik.

Konponbidea:

Schneider Electric-ek ahultasun hori konpondu egin du ZelioSoft2 v5.2 bertsioan.

Xehetasuna:

- Bereziki aldatutako fitxategi bat erabiliz, erasotzaile batek urrunetik kodea exekutatzea lor lezake, askatutako memoriarako erreferentzien egiaztapenean dagoen akats bat baliatuz. Ahultasun horretarako CVE-2018-7817 identifikatzailea erreserbatu da.

Etiketak: Schneider Electric, Ahultasuna