2018ko Ekainaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Hainbat ahultasun GEren MDS PulseNETen

Argitalpen data: 2018/06/01

Garrantzia: Handia

Kaltetutako baliabideak:

- MDS PulseNETen 3.2.1 bertsioa eta lehenagokoak
- MDS PulseNET Enterpriseren 3.2.1 bertsioa eta lehenagokoak

Azalpena:

Rgod ikerlariak hainbat ahultasunen berri eman dio Zero Day Initiative-ri (ZDI). Ahultasun horiek GEren MDS PulseNET eta MDS PulseNET Enterprise-ri eragiten diete eta hainbat eratakoak dira: autentifikazio okerra, kanpoko entitateko XML erreferentziako murrizpen ezegokia, eta bide transbertsal erlatiboa. Ahultasun horiek baliatuz erasotzaile batek pribilegioen igoera edo informazioaren exfiltrazioa lor litzake.

Konponbidea:

GEk PulseNET produktuaren softwarea eta arkitektura aldatu ditu. Azken bertsioak ahultasun horiek konpontzen ditu. GEk erabiltzaileei aholkatzen die PulseNET 4.1 bertsiora edo geroagoko batera eguneratzea ahultasun horiek konpontzeko.

PulseNETen eguneraketak hemen eskura daitezke:

http://www.gegridsolutions.com/Communications/MDS/PulseNET_Download.aspx

PulseNET Enterpriseren eguneraketak hemen eskura daitezke:

http://www.gegridsolutions.com/Communications/MDS/PulseNETEnt_Download.aspx

Xehetasuna:

- Egiaztatze okerra: baimenik gabeko erasotzaile batek Java Remote Proper Invocation-en (RMI) sarrera ataka balia lezake aplikazioak abiatzeko eta urruneko kodea exekutatzen laguntzeko Web zerbitzuen bidez. Ahultasun horretarako CVE-2018-10611 identifikatzailea erabili da.
- Kanpoko entitateko XML erreferentziako murrizpen ezegokia: erasotzaile batek XML External Entity (XXE) erako erasoen hainbat aldagai balia litzake Windows plataformatik datuak exfiltratzeko. Ahultasun horretarako CVE-2018-10613 identifikatzailea erabili da.
- Bide erlatiboaren saltoa: erasotzaile batek direktorio salto bat balia lezake exfiltrazio bat edo fitxategien ezabaketa eragiteko plataforman. Ahultasun horretarako CVE-2018-10615 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Delta Electronics-en Delta Industrial Automation DOPSoft-en

Argitalpen data: 2018/06/01

Garrantzia: Handia

Kaltetutako baliabideak:

- DOPSoft-en 4.00.04 bertsioa eta lehenagokoak.

Azalpena:

B0nd @garagehackers ikerlaria, Trend Micro-ko Zero Day Initiative-rekin elkarlanean, bufferraren gainezkatzea eta mugez kanpoko irakurketa erako ahultasunak aurkitu ditu Delta Electronics-en Delta Industrial Automation DOPSoft-en. Urruneko erasotzaile batek

informazio konfidentziala irakur lezake, kode arbitrarioa exekutatu edota aplikazioaren erorketa eragin.

Konponbidea:

Delta Electronicsek erabiltzaile kaltetuei gomendatzen die azken bertsiora eguneratzea, hemen eskuragarri:

http://www.deltaww.com/Products/PluginWebUserControl/downloadCenterCounter.aspx?DID=9063&DocPath=1&hl=en-US

Delta Electronicsek, era berean, kaltetutako erabiltzaileei gomendatzen die aplikazioaren interakzioa konfiantzako fitxategietara mugatzea.

Xehetasuna:

- Mugez kanpoko irakurketa: Aplikazioak memoria buffer baten irakurketa eragiketak ezartzen ditu eta horietan kokapena zein den jakin daiteke .dpa fitxategi bateko balio bat irakurriz. Horrek memoriaren bufferraren mugen barnean eragiketen mugaketa desegokia eragin lezake, hainbat gertakari ahalbidetuz: urruneko kodea exekutatzea, aurreikusitako kontrol fluxua aldatzea, informazio konfidentziala irakurtzea edo aplikazioaren erorketa eragitea. Ahultasun horretarako CVE-2018-10623 identifikatzailea erabili da.
- Bufferrak gainezka egitea: Aplikazioak luzera finkoko buffer bat erabiltzen du eta pilaren bufferraren luzera baino handiagoko balio bat .dpa fitxategi batetik irakur daiteke, bufferra gainidaztea eraginez. Horren ondorioz, urrunetik kodea exekuta liteke eta aplikazioaren erorketa eragin. Ahultasun horietarako CVE-2018-10617 eta CVE-2018-10621 identifikatzaileak erabili dira.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Schneider Electric-en U.motion Builder-en

Argitalpen data: 2018/06/04

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- U.motion Builder-en 1.3.4 bertsioa baino lehenagoko guztiak

Azalpena:

 eta Wei Gao-k (Ixia A Keysight Business) hainbat ahultasunen berri eman diote Schneider Electric-i. Horiek baliatuz erasotzaile batek kode arbitrarioa exekuta lezake, memoriaren bufferra irakurri, segmentazio akatsa eragin edo autentifikazioa saihestu.

Konponbidea:

Schneider Electricek ahultasun horiek konpontzen dituen 1.3.4 bertsioa argitaratu du, eta hemen dago eskuragarri:

- https://www.schneider-electric.com/en/download/document/Umotion_Server_update/

Xehetasuna:

Aurkitutako ahultasunak honakoak dira:

- Sarrera datuak ez balioztatzea: Ahultasun hau gertatzen da aplikazioak sarrera datuak komando baten modura ebaluatzen dituenean. Hartara, erasotzaile batek kode arbitrarioa exekuta lezake, memoriaren bufferra irakurri edo aplikazioaren segmentazioan akats bat eragin. Larritasun kritikoko ahultasun horretarako CVE-2018-7784 identifikatzailea erabili da.
- Autentifikazioari ihes egitea: Urruneko komando baten injekzioaren bidez autentifikazioari ihes egitea lor daiteke. Larritasun kritikoko ahultasun horretarako CVE-2018-7785 identifikatzailea erabili da.
- Cross-Site-Scripting ("XSS"): Cross-Site-Scripting ("XSS") erako ahultasun bat baliatuz erasotzaile batek script gaiztoak injekta litzake. Larritasun ertaineko ahultasun horretarako CVE-2018-7786 identifikatzailea erabili da.
- Sarrera datuen balioztatze ezegokia: Ahultasun honen iturburua HTTP GET eskaera batean sarrera datuen balioztatze ezegokia da. Larritasun ertaineko ahultasun horretarako CVE-2018-7787 identifikatzailea erabili da.

Etiketak: Eguneraketa, Schneider Electric, Ahultasuna

Hainbat ahultasun Philips-en IntelliVue Patient Monitors eta Avalon Fetal/Maternal Monitors-en

Argitalpen data: 2018/06/06

Garrantzia: Handia

Kaltetutako baliabideak:

- IntelliVue Patient Monitors MP Series (MP2/ X2/ MP30/ MP50/ MP70/ NP90/ MX700/ 800) Rev B-M
- IntelliVue Patient Monitors MX (MX400-550) Rev J-M (X3/MX100, soilik Rev M)
- Avalon Fetal/Maternal Monitors FM20/FM30/FM40/FM50, F.0, G.0 eta J.3 Berrikuspenak

Azalpena:

Medigate-ko Oran Avraham-ek, Philipsekin koordinazioan, ahultasun hauen berri eman dio NCCICri. Ahultasun hauek arrakastaz baliatuz gero, erasotzaile batek memoria irakur/idatz lezake edota zerbitzuaren ukapen egoera sortu sistema berrabiaraziz. Horrek pazienteen diagnostikoan eta tratamenduan atzerapena eragin lezake.

Konponbidea:

Philipsek zuzenketa partxe bat eskainiko du bertsio berezietarako, bai eta eguneraketa bat ere bertsio guztietarako.

Philipsek ondoko arintzeak eskaini ditu ahultasun horietarako:

- Philipsek aholkatzen du kaltetutako gailuaren argibideak jarraitzea. Philipsek 2018an konponbideak eskainiko ditu partxe modura IntelliVue-ren J-M berrikuspenetarako eta Avalon-en G.0 eta J.3 berrikuspenetarako. IntelliVueren bertsio zaharragoak dituzten erabiltzaileei Philipsek eguneraketa bide bat eskainiko die euskarria duten berrikuspenetarako. Eguneraketa aukeretarako, erabiltzaileak harremanetan jarri behar dira Philipseko beren salmenta ordezkariarekin.
- IntelliVue Monitorsen kasuan, Philipsek erabiltzaileei gomendatzen die segurtasun fisiko eta logikoko erabilera argibideak jarraitzea (Kliniketako sareen gidarako Segurtasuna). Modu osagarrian, Philipsek erabiltzaileei gomendatzen die K.2 edo geroagoko berrikuspenetara eguneratzea.
- Avalon Fetal Monitor-en G.0 eta J.3 bertsioetarako Philipsek erabiltzaileei aholkatzen die instalazio eta zerbitzu gidaliburua jarraitzea (Datuen Pribatutasuna eta Sarearen Segurtasunerako Baldintzak).
- Avalon Fetal Monitor F.0ren kasuan Philipsek erabiltzaileei aholkatzen die argibideak jarraitzea, Datuen Pribatutasuna eta Sarearen Segurtasunerako Baldintzen zerbitzu Gidako Rev J.3 atalean zehazten den moduan.
- IntelliVue eta Avalon Fetal Monitor-en instalazio bereziak dituzten erabiltzaileen zalantzak argitzeko, Philipsek gomendatzen du bakoitza bere laguntza zerbitzu lokalarekin harremanetan jartzea edo bestela eskualdeko laguntza zerbitzuarekin.

Xehetasuna:

- Egiaztatze okerra: Ahultasun honi esker baimenik gabeko erasotzaile batek memoriara sarbidea lor lezake azpisare beraren barnean erasotzaileak berak aukeratutako gailu baten helbidetik. Larritasun altuko ahultasun horretarako CVE-2018-10597 identifikatzailea erabili da.
- Informazioaren agerpena: Ahultasun honi esker baimenik gabeko erasotzaile batek memoria irakur lezake azpisare beraren barnean erasotzaileak berak aukeratutako gailu baten helbidetik. Larritasun ertaineko ahultasun horretarako CVE-2018-10599 identifikatzailea erabili da.
- Pilan oinarritutako buffer gainezkatzea: Ahultasun honek "echo" zerbitzu bat agerian uzten du. Hori baliatuz, erasotzaile batek buffer bat bidal lezake azpisare berean berak hautatutako gailu baten helbide batera, bufferra pilara kopiatuko litzateke mugen egiaztapenik gabe, eta pilaren gainezkatzea eragingo litzateke. Larritasun altuko ahultasun horretarako CVE-2018-10601 identifikatzailea erabili da.

Etiketak: Ahultasuna

Ahultasuna Rockwell Automation-en RSLinx Classic eta FactoryTalk Linx Gateway-n

Argitalpen data: 2018/06/08

Garrantzia: Handia

Kaltetutako baliabideak:

- RSLinx Classic, 3.90.01 bertsioa eta lehenagokoak.
- FactoryTalk Linx Gateway, 3.90.00 bertsioa eta lehenagokoak.

Azalpena:

Zero Science Lab-eko Gjoko Krstic-ek, Rockwell Automationekin batera, ahultasun honen berri eman dio NCCICri. Hori baliatuz baimenak dituen baina pribilegiorik ez duen erasotzaile lokal batek kode arbitrarioa exekuta lezake eta erabiltzailearen pribilegioen eskalatzea ere egin lezake kaltetutako lanpostuan.

Konponbidea:

- RSLinx Classic-en 3.90.01 bertsioaren eta lehenagokoen kasuan, 4.00.01 bertsiora edo berriagoetara eguneratzea, hemen eskuragarri: https://compatibility.rockwellautomation.com/Pages/MultiProductDownload.aspx?crumb=112
- FactoryTalk Linx Gatewayren 3.90.00 bertsioaren eta lehenagokoen kasuan, 6.00.00 bertsiora edo berriagoetara eguneratzea, hemen eskuragarri: https://compatibility.rockwellautomation.com/Pages/MultiProductDownload.aspx?crumb=112

Xehetasuna:

Entrekomillatu gabeko elementu baten edo bilaketa bide baten moduko ahultasun bat baliatuz, baimenak dituen baina pribilegiorik ez duen erasotzaile lokal batek kode arbitrarioa exekuta lezake, eta erabiltzailearen pribilegioen eskalatzea ere egin lezake kaltetutako lanpostuan. Ahultasun horretarako CVE-2018-10619 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Siemensen produktuetan

Argitalpen data: 2018/06/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- RAPIDLab 1200, RAPIDPoint 400 eta RAPIDPoint 500 sistemak, Siemens Healthineers Informatics produktuak erabiltzen ez dituzten bertsio guztiak.
- RAPIDLab 1200 Series, Siemens Healthineers Informatics produktuekin 3.3 bertsioa baino lehenagoko guztiak.
- RAPIDPoint 500 sistemak: 3.0 bertsioa eta ondorengoak, 2.4.X bertsioa eta 2.3 bertsioa eta lehenagokoak Siemens Healthineers Informatics produktuekin.
- RAPIDPoint 400 sistemak: bertsio guztiak Siemens Healthineers Informatics produktuekin.
- RFID 181-EIP bertsio guztiak.
- RUGGEDCOM WiMAX, 4.4 eta 4.5 bertsioak.
- SCALANCE X-200, 5.2.3 bertsioa baino lehenagokoak.
- SCALANCE X-200 IRT, 5.4.1 bertsioa baino lehenagokoak.
- SCALANCE X-204RNA, bertsio guztiak.
- SCALANCE X-300, bertsio guztiak.
- SCALANCE X408, bertsio guztiak.
- SCALANCE X414, bertsio guztiak.
- SIMATIC RF182C, bertsio guztiak.

- SCALANCE X-200, 5.2.3 bertsioa baino lehenagokoak.
- SCALANCE X-200 IRT, 5.4.1 bertsioa baino lehenagokoak.
- SCALANCE X-300, bertsio guztiak.
- SCALANCE M875, bertsio guztiak.
- License Management System (LMS), 2.1 eta lehenagoko bertsioak.
- Annual Shading, 1.0.4 eta 1.1 bertsioak.
- Desigo AVT, 3.1.0, 3.0.1 eta lehenagoko bertsioak (builds 12.10.318, 12.0.850.0, 11.10.55.0, 11.0.360.0, 10.10.845.0 eta 10.0.830.0).
- Desigo CC / Cerberus DMS, 1.1, 2.0, 2.1 eta 3.0 bertsioak.
- Desigo Configuration Manager (DCM), 6.1 SP2 bertsioa eta lehenagokoak, 6.0 SP1 eta lehenagokoak.
- Desigo XWP, 6.1 bertsioa eta lehenagokoak.
- SiteIQ Analytics, 1.1, 1.2 eta 1.3 bertsioak.
- Siveillance Identity, 1.1 bertsioa.

Azalpena:

Siemens produktuetan 14 ahultasun aurkitu dira guztira, horietako bat larritasun kritikokoa, zortzi larritasun altukoak eta bost ertainekoak.

Konponbidea:

- RAPIDLab 1200, RAPIDPoint 400 eta RAPIDPoint 500 sistemetarako, Siemens Healthineers Informatics produktuak erabiltzen ez dituzten bertsio guztiak:
  - Sarbide fisikoa langile baimenduek soil-soilik izatea.
  - "Remote Viewing" ezaugarria desgaitzea, Operadoreen Gidako "Enabling or Disabling Remote Viewing" ataleko argibideak jarraituz.
- RAPIDLab 1200 Series-en kasuan, Siemens Healthineers Informatics produktuekin 3.3 bertsioa baino lehenagoko guztiak:
  - Sarbide fisikoa langile baimenduek soil-soilik izatea.
  - 3.3 edo 3.3.1 bertsioetara eguneratzea.
  - Pasahitza aldatzea.
  - RAPIDComm® Data Management System-ekin konektagarritasun segurua bermatzeko, RAPIDComm® V7.0 edo goragoko bertsioa erabiltzea gomendatzen da.
- RAPIDPoint 500 sistemetarako, 3.0 bertsioa eta ondorengoak, 2.4.X bertsioa eta 2.3 bertsioa eta lehenagokoak Siemens Healthineers Informatics produktuekin:
  - Sarbide fisikoa langile baimenduek soil-soilik izatea.
  - Pasahitza aldatzea.
  - RAPIDComm-ekin konektagarritasun segurua bermatzeko, RAPIDComm V7.0 edo goragoko bertsioa erabiltzea gomendatzen da.
- RAPIDPoint 400 sistemen bertsio guztietarako Siemens Healthineers Informatics produktuekin:
  - Sarbide fisikoa langile baimenduek soil-soilik izatea.
  - RAPIDPoint 500 seriera eguneratzea.
  - Eguneratzea posible ez bada, "Remote Viewing" ezaugarria desgaitzea gomendatzen da, Operadoreen Gidako "Enabling or Disabling Remote Viewing" ataleko argibideak jarraituz.
- RFID 181-EIP, SIMATIC RF182C, SCALANCE-X-204RNA, SCALANCE X-300, SCALANCE X408, eta SCALANCE X414 ekipoen bertsio guztietarako, bai eta Ruggedcom Wimax-en 4.4 eta 4.5 bertsioetarako:
  - IP helbide estatikoak erabiltzea, DHCP ordez.
  - Gelaxkaren babesa kontzeptua aplikatzea (adibidez, switchetan "port security" aplikatzea).
  - Defentsa sakoneko estrategiak aplikatzea.
- SCALANCE X-200 kommutadorearen 5.2.3 bertsioa baino lehenagokoetarako:
  - Firmwarea 5.2.3 bertsiora eguneratzea.
- SCALANCE X-200 IRT kommutadorearen 5.4.1 bertsioa baino lehenagokoetarako:
  - Firmwarea 5.4.1 bertsiora eguneratzea.
- SCALANCE X-200 kommutadorearen 5.2.3 bertsioa baino lehenagokoetarako:
  - Firmwarea 5.2.3 bertsiora eguneratzea.
- SCALANCE X-200 IRT kommutadorearen 5.4.1 bertsioa baino lehenagokoetarako:
  - Firmwarea 5.4.1 bertsiora eguneratzea.
- SCALANCE X300 kommutadorearen bertsio guztietarako:
  - Kaltetutako gailuek sarera duten sarbidea babestea.
- SCALANCE M875en bertsio guztietarako:
  - Hardwarea eguneratzea SCALANCE M876-4 edo RUGGEDCOM RM1224 modeloetara.
  - Firmwarea eguneratzen ez den bitartean, web kudeaketaren interfazerako sarbidea barneko sareetara edo VPNetara soilik mugatzea gomendatzen da, eta horrez gain produktuak serietik lehenetsita dakarren suebakia erabiltzea web interfazerako sarbidea IP fidagarriek soilik izan dezaten, erabiltzaile administratzailearen kontua pasahitz sendoekin babestea, eta beste orrialde batzuetan ez nabigatzea edo kanpoko loturetan ez klikatzea administrazioaren web interfazea autentifikatzen ari den bitartean.
- License Management System-en (LMS) 2.1 eta lehenagoko bertsioetarako:
  - Dongle driver-a eguneratzea, Siemensen webean azaltzen diren argibideak jarraituz.
- Annual Shading-en 1.0.4 eta 1.1 bertsioetarako:
  - Dongle driver-a eguneratzea, Siemensen webgunean azaltzen diren argibideak jarraituz.
- Desigo AVTren 3.1.0, 3.0.1 eta lehenagoko bertsioetarako (builds 12.10.318, 12.0.850.0, 11.10.55.0, 11.0.360.0, 10.10.845.0 eta 10.0.830.0):
  - Dongle driver-a eguneratzea, Siemensen webgunean azaltzen diren argibideak jarraituz.
- Desigo CC / Cerberus DMSren 1.1, 2.0, 2.1 eta 3.0 bertsioetarako:
  - Dongle driver-a eguneratzea, Siemensen webgunean azaltzen diren argibideak jarraituz.
- Desigo Configuration Manager-en (DCM) 6.1 SP2 bertsioa eta lehenagokoak eta 6.0 SP1 eta lehenagokoetarako:
  - Dongle driver-a eguneratzea, Siemensen webgunean azaltzen diren argibideak jarraituz.
- Desigo XWPren 6.1 bertsioa eta lehenagokoetarako:
  - Dongle driver-a eguneratzea, Siemensen webgunean azaltzen diren argibideak jarraituz.
- SiteIQ Analytics-en 1.1, 1.2 eta 1.3 bertsioetarako:
  - Dongle driver-a eguneratzea, Siemensen webgunean azaltzen diren argibideak jarraituz.
- Siveillance Identity 1.1en bertsioetarako:
  - Dongle driver-a eguneratzea, Siemensen webgunean azaltzen diren argibideak jarraituz.

Xehetasuna:

- Urruneko erasotzaile batek "Remote View" ezaugarrira sarbide urrunekoa edo lokala izateko kredentzialak izango balitu, bere pribilegioak igo litzake, eta sistemaren konfidentzialtasuna, integritatea eta eskuragarritasuna arriskuan jarri. Larritasun altuko ahultasun horretarako CVE-2018-4845 identifikatzailea erreserbatu da.
- Pasahitza barneratua duen fabrikako kontu bat baliatuz, erasotzaileek gailurako sarbidea izan lezakete TCP 5900 atakan barrena, sistemaren konfidentzialtasuna, integritatea eta eskuragarritasuna arriskuan jarriz. Larritasun altuko ahultasun horretarako CVE-2018-4846 identifikatzailea erreserbatu da.
- Pribilegiorik gabeko urruneko erasotzaile bat kaltetutako gailuak dauden sare segmentu berberean lokalki kokatuko balitz, gailu horietan kodea exekuta lezake urrunetik DHCP erantzunak bidaliz, modu berezian manipulatuak bezero baten DHCP eskarien aurrean. Larritasun altuko ahultasun horretarako CVE-2018-4833 identifikatzailea erreserbatu da.
- Web interfazera (443/tcp) sarbidea lukeen urruneko erasotzaile autentifikatu batek sistema eragilearen komandoak exekuta litzake

modu arbitrarioan. Larritasun altuko ahultasun horietarako CVE-2018-4859 eta CVE-2018-4860 identifikatzaileak erreserbatu dira.
- 443/tcp atakaren web interfazea baliatuz Cross-Site Request Forgery (CSRF) motako eraso bat gerta liteke, erabiltzaile bat ustekabean harrapatu eta engainatuz gero gurpil gaizto batera sar dadin. Larritasun altuko ahultasun horretarako CVE-2018-11447 identifikatzailea erreserbatu da.
- Autentifikatu gabeko erasotzaile batek zerbitzuaren ukapena (DoS) eragin lezake erabiltzailearen interakzioaren beharrik gabe. Larritasun altuko ahultasun horretarako CVE-2018-6304 eta CVE-2018-6305 identifikatzaileak erreserbatu dira.
- Autentifikatu gabeko erasotzaile batek kodea injekta lezake Admin Control Center-eko logen orrian. Kodea exekutatzen da erabiltzaile administrari batek orrialde kaltetua bisitatzen duenean. Horrek sistemaren konfidentzialtasun, integritate eta eskuragarritasunean eragin dezake. Larritasun kritikoko ahultasun horretarako CVE-2018-8900 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Siemens, Ahultasuna

Hainbat ahultasun Natus Medical-en Xltek NeuroWorks-en

Argitalpen data: 2018/06/15

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Natus Xltek NeuroWorks 8. bertsioa

Azalpena:

Cisco Talos-eko Cory Duplantis-ek aurkitu ditu Natusen ahultasun hauek eta horien berri eman du. Ahultasun horiek arrakastaz baliatzeko Natuseko bezeroen sarera sarbidea izan beharra dago, eta kasu horretan sarbidea lortzen den gailua blokea liteke. Bufferraren gainezkatzearen egoera batean urruneko kodea exekuta liteke.

Konponbidea:

Natusek NeuroWorks/SleepWorks 8.5 GMA 3 argitaratu du, NeuroWorks/SleepWorks 8ren ahultasunak konpontzen dituzten segurtasun hobekuntzak dituen software eguneraketa.Eguneraketa eskuragarri dago NeuroWorks/SleepWorks 8.0, 8.1, 8.4 eta 8.5 bertsioen erabiltzaileentzat.Konponbidea behar baduzu, jar zaitez harremanetan Natus Neuroren laguntza teknikorako departamentuarekin 1-800 387-7516 telefono zenbakian edo mezu bat bidali helbidera xehetasun gehiago lortzeko.

Xehetasuna:

- Bereziki diseinatutako pakete batek mugez kanpoko irakurketa eragin dezake, eta horren ondorioz zerbitzuaren ukapen egoera gerta daiteke. Ahultasun horietarako CVE-2017-2852, CVE-2017-2858, CVE-2017-2860 eta CVE-2017-2861 identifikatzaileak erreserbatu dira.
- Erasotzaile batek bufferraren gainezkatzea eragin dezake kaltetutako produktura bereziki diseinatutako pakete bat bidaliz, produktua bezeroak eskatutako fitxategia irekitzen saiatzen ari den bitartean. Ahultasun horretarako CVE-2017-2853 identifikatzailea erreserbatu da.
- Komando jakin batzuk exekutatzen ari direnean jasotzen den bereziki diseinatutako pakete batek eragin lezake memoria modu berezi batean gainidaztea, eta horren bitartez erasotzaileak programaren kontrola eskura lezake. Ahultasun horretarako CVE-2017-2867 identifikatzailea erreserbatu da.
- Datuen egiturak aztertzeko moduan programak duen akats baten ondorioz erasotzaile batek sistemaren kontrola eskura lezake, bereziki diseinatutako pakete bat bidaliz. Ahultasun horretarako CVE-2017-2868 identifikatzailea erreserbatu da.
- Datuen egitura aztertzeko programak duen modua balia dezake bereziki diseinatutako pakete batek eta bufferraren gainezkatzea eragin, kode arbitrarioa urrunetik exekutatzea ahalbidetuz. Ahultasun horretarako CVE-2017-2869 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

DLLren bahiketa ABBren Pluto Manager-en

Argitalpen data: 2018/06/19

Garrantzia: Ertaina

Kaltetutako baliabideak:

- Pluto Manager, 2.24-2.34.3 bertsioak

Azalpena:

Herman Groeneveld ikerlari independenteak DLLren bahiketa erako ahultasuna aurkitu du ABBren Pluto Manager aplikazioan. Erasotzaile lokal batek kode gaiztoa exekuta lezake aplikazioaren pribilegio berdinekin.

Konponbidea:

- Ahultasun hori konpontzeko ABBk Pluto Manager-en 2.36 bertsioa argitaratu du.

Xehetasuna:

Erasotzaile lokal batek DLL gaizto bat berrizenda lezake aplikazioak karga lezan, kargatutako DLLen zuzentasuna ez baita egiaztatzen. Aplikazioak DLLa kargatzen duenean, aplikazioaren pribilegio berdinekin exekutatuko da kode gaiztoa.

Etiketak: Eguneraketa, Ahultasuna

Bufferra gainezkatzea Delta Electronics-en Delta

Industrial Automation COMMGRn

Argitalpen data: 2018/06/22

Garrantzia: Handia

Kaltetutako baliabideak:

- COMMGR 1.08 bertsioa eta lehenagokoak
  - DVPSimulator EH2, EH3, ES2, SE, SS2
  - AHSIM_5x0, AHSIM_5x1

Azalpena:

Trend Microren Zero Day Initiativerekin lanean ari zen ikerlari anonimo batek bufferraren gainezkatze bat identifikatu du, Delta Electronics-en Delta Industrial Automation COMMGRen komunikazio kudeatzailearen softwareari eragiten diona. Urruneko erasotzaile batek urruneko kodea exekutatzea lor lezake, eta aplikazioak huts egitea edo aplikazioaren zerbitzarian zerbitzu ukazioa gertatzea.

Konponbidea:

Delta Electronicsek softwarearen v1.09 bertsioa argitaratu du, ahultasun hori konpontzen duena. Bertsio hori lotura honetan aurki daiteke: http://www.deltaww.com/Products/PluginWebUserControl/downloadCenterCounter.aspx?DID=2093&DocPath=1&hl=en-US

Delta Electronicsek zerrenda zuriak aplikatzea ere gomendatzen du, 502 eta 10002 ataken gainean komunikazio baimenduak soilik ahalbidetzeko.

Xehetasuna:

Aplikazioak luzera finkoko bufferra erabiltzen du, eta bertan luzera definitu gabe duen balio bat sareko paketeek irakur dezakete sare ataka berezi baten bidez, bufferra gainidaztea eraginez. Horrek ahalbidetzen du kodearen urruneko exekuzioa, aplikazioak huts egitea, edo aplikazioaren zerbitzarian zerbitzuaren ukazioa gertatzea. Ahultasun horretarako CVE-2018-10594 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Sarrera eremuen balioztatze ezegokia Rockwell Automation-en produktuetan

Argitalpen data: 2018/06/22

Garrantzia: Handia

Kaltetutako baliabideak:

- Allen-Bradley CompactLogix 5370 L1, L2 eta L3, 30.012 bertsioa eta lehenagokoak.
- Allen-Bradley Armor CompactLogix 5370 L3, 30.012 bertsioa eta lehenagokoak.
- Allen-Bradley Compact GuardLogix 5370, 30.012 bertsioa eta lehenagokoak.
- Allen-Bradley Armor Compact GuardLogix 5370, 30.012 bertsioa eta lehenagokoak.

Azalpena:

Applied Risk-eko Alexey Perepechkok sarrera eremuen balioztatze ezegoki motako ahultasun bat identifikatu du, Rockwell Automationen hainbat produktu kaltetzen dituena, eta zerbitzuaren ukazioa eragin lezakeena.

Konponbidea:

Rockwell Automationek kaltetutako erabiltzaileei aholkatzen die eragindako produktuak firmwarearen FRN berrikuspenera eguneratzea (31.011 edo geroagokoa). Firmwarea ondoko loturan dago eskuragarri:
https://compatibility.rockwellautomation.com/Pages/MultiProductDownload.aspx?crumb=112

Era berean, ondoren aipatzen diren prebentzio neurriak hartzea gomendatzen du:

- Fabrikazio zonaren kanpotik Ethernet / IPrako edo CIP protokoloan oinarritutako beste gailu batzuetarako trafiko guztia blokeatzea, 2222 eta 44818 / TCP eta UDP ataketarako sarbidea blokeatuz edo murriztuz, sare azpiegitura egokia erabiliz, esate baterako suebakiak, UTM gailuak edo segurtasuneko beste gailu batzuk. Rockwell Automation Products-ek erabiltzen dituen TCP / UDP atakei buruzko informazio gehiago eskuratzeko irakurri jakintza baseko ID 898270 artikulua, hemen eskuragarri: https://rockwellautomation.custhelp.com/app/answers/detail/a_id/898270/page/1
- Sarearen esposizioa murriztea kontrol gailu edota sistema guztientzat, eta Internetetik sarbiderik ez dutela ziurtatzea.
- Urruneko sarbidea behar denean, metodo seguruak erabiltzea, esate baterako Sare Pribatu Birtualak (VPN).

Xehetasuna:

Balizko erasotzaile batek TCP pakete berezi bat bidal lezake eta akats garrantzitsu ez berreskuragarri bat (MNRF) sortu, zerbitzuaren ukazioa eraginez. Ahultasun horretarako CVE-2017-9312 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Sarbidearen kontroleko hainbat ahultasun Siemensen produktu batzuetan

Argitalpen data: 2018/06/26

Garrantzia: Ertaina

Kaltetutako baliabideak:

- IEC 61850 system configurator, V5.80 bertsioa baino lehenagoko guztiak
- DIGSI 5, V7.80 bertsioa baino lehenagoko guztiak
- DIGSI 4, bertsio guztiak
- SICAM PAS/PQS, V8.11 bertsioa baino lehenagoko guztiak
- SICAM PQ Analyzer, V3.11 bertsioa baino lehenagoko guztiak
- SICAM SCC, bertsio guztiak

Azalpena:

Atredis Partners-eko Chris Bellows eta HD Moore eta San Diego Gas and Electric-eko Austin Scottek eman diote Siemensi ahultasun hauen berri. Kaltetutako produktuen ahultasun honek erasotzaile bati ahalbidetu liezaioke sistemaren datu mugatuak filtratzea edo kodea exekutatzea sistema eragilearen erabiltzailearen baimenekin.

Konponbidea:

Siemensek ondoko neurriak proposatzen ditu kaltetutako produktu bakoitzerako:

- IEC 61850 system configurator: V5.80 bertsiora eguneratzea, hemen eskuragarri: https://support.industry.siemens.com/cs/ww/en/view/109740546
- DIGS 5: IEC 61850 system configurator desinstalatzea edo V7.80 bertsiora eguneratzea, hemen eskuragarri: https://support.industry.siemens.com/cs/ww/en/view/109758531
- SICAM PAS/PQS: V8.11 bertsiora eguneratzea, hemen eskuragarri: https://support.industry.siemens.com/cs/us/en/view/109757831
- SICAM PQ Analyzer: V3.11 bertsiora eguneratzea, hemen eskuragarri: https://support.industry.siemens.com/cs/us/en/view/109757833
- DIGSI 4 y SICAM SCC: Suebakiaren konfigurazioa aldatzea TCP 4884, 5885 eta 5886 ataketarako sarbidea mugatzeko localhostari (kaltetutako produktuaren arabera) Horrez gain, azpiestazio seguruen segurtasun ildoak jarraitzea, hemen eskuragarri:n https://www.siemens.com/gridsecurity

Xehetasuna:

Kaltetutako produktuetan TCP 4884, 5885 eta 5886 ataketako hostaren sareko interfaze guztietan entzuten duen zerbitzu batek erasotzaile bati ahalbidetu liezaioke sistemaren datu mugatuak filtratzea edo kodea exekutatzea Microsoft Windowseko erabiltzaile baimenekin.

Ahultasuna arrakastaz baliatzeko erasotzaileak kaltetutako zerbitzura bereziki diseinatutako sare eskaria bidaltzea lortu behar du, bai eta erabiltzaile batek zerbitzuaren aplikazio bezeroarekin anfitrioian interaktuatzea ere. Microsoft Windowseko erabiltzaile baimenekin kode arbitrarioa exekutatzeko, erasotzaile batek kodea anfitrioian ezartzeko gai izan behar du, aldez aurretik eta beste bide batzuen bitartez. Ahultasun horretarako CVE-2018-4858 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Siemens, Ahultasuna

Hainbat ahultasun Medtronic-en MyCareLink Patient Monitor-en

Argitalpen data: 2018/06/29

Garrantzia: Ertaina

Kaltetutako baliabideak:

- 24950 MyCareLink Monitor, bertsio guztiak
- 24952 MyCareLink Monitor, bertsio guztiak

Azalpena:

Clever Securityko Peter Morganek Medtronicen MyCareLink Patient Monitor-en produktu batzuei eragiten dieten hainbat ahultasunen berri eman du. Sarbide fisikoa lukeen balizko erasotzaile batek monitorearen sistema eragilera sartzeko baimena lor lezake, eta memoriako balio arbitrarioak irakurri eta idatz litzake.

Konponbidea:

Medtronicek produktu eguneraketa batzuk argitaratuko ditu, ohartarazpen honetan azaltzen diren ahultasunak murriztearren. Eguneraketa hauek automatikoki aplikatuko dira gailuetan, eguneraketen prozesu estandar errepikarien parte modura. Horrez gain, kaltetutako gailuen eta horiekin lotutako azpiegituraren segurtasunaren monitorizazioa areagotu egin du Medtronicek.

Medtronicek erabiltzaileei aholkatzen die babes neurri osagarriak hartzea, ahultasun hauek baliatzeko arriskua murriztearren. Zehazki, erabiltzaileek honakoa egin behar lukete:

- Etxeko monitorearen gaineko kontrol fisiko egokiak mantentzea, hori baita ahultasunak murrizteko erarik onena.
- Soilik osasun arretako hornitzailearen edo Medtroniceko ordezkari baten aldetik eskuratutako etxeko monitoreak erabiltzea, sistemaren integritatea bermatzearren.
- Osasun arretako hornitzaileari edo Medtroniceko ordezkariari jakinaraztea etxeko monitorearekin zerikusia duen edozein jokabide.

Medtronicek argitaratutako informazio gehiago ondoko loturan aurki daiteke: https://www.medtronic.com/security

Xehetasuna:

- Kaltetutako produktuek sistema eragilearen pasahitzak dauzkate barnean. Sarbide fisikoa lukeen balizko erasotzaile batek gailuaren karkasa ireki lezake, debug atakara konektatu eta pasahitza erabili sistema eragilera sarbide baimendua lortzeko. Ahultasun horretarako CVE-2018-8870 identifikatzailea erabili da.
- Kaltetutako produktuek arazketa kodea daukate, monitorearen komunikazio interfazeen funtzionaltasunak probatu ahal izateko, monitorearen eta ezar daitekeen bihotzeko gailuaren arteko interfazearenak barne. Balizko erasotzaile batek ahultasun hau balia lezake bihotzeko gailu ezargarrietan memoria balio arbitrarioak irakurri eta idazteko, haririk gabeko indukzio protokoloen edo irispide laburrekoen bidez. Ahultasun horretarako CVE-2018-8868 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna