
# 2018ko Apirilaren Bulletina

## Ohartarazpenak - Kontrol Industrialeko Sistemak

## Hainbat ahultasun Philips-en iSite eta IntelliSpace PACSen

**Argitalpen data:** 2018/04/02

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

iSite eta IntelliSpace PACSen bertsio guztiak.

**Azalpena:**

Philipsek hainbat ahultasunen berri eman du, baliatuak izateko zailtasun baxukoak, eta erasotzaile bati ondoko ekintzak egitea ahalbidetuko lioketenak: aplikaziora ustekabeko sarrerak bidaltzea, kode arbitrarioa exekutatzea, sistemaren kontrolaren fluxua aldatzea, informazio sentikorra eskuratzea edo sistemaren ustekabeko itxiera eragitea. Horrelakoen bidez pazientearen konfidentzialtasuna, sistemaren integritatea edota bere eskuragarritasuna arriskuan jarriko lirateke.

**Konponbidea:**

Philips IntelliSpace PACS arriskua murrizten duen ingurune kontrolatu batean exekutatzen da (VPN erabiliz, sare isolatu batean firewall bidez eta interneterako sarbiderik gabe). Horrez gain, Philipsek bere sistemetako mehatxuak monitorizatu eta kudeatzen dituen antibirus bat dauka.

Prebentzio neurri modura, Philipsek ondokoa gomendatzen du:

- Philipsen partxeen programa iraunkorrean izena ematea
- Sistemaren firmwarea eguneratzea
- IntelliSpace PACS 4.4.55x-era eguneratzea Windows 2012 sistema eragilearekin

Era berean, erabiltzaileen eskura dauka bezeroaren arreta zerbitzu bat kontsultak egin ahal izateko. Hemen dago eskuragarri:

- https://www.usa.philips.com/healthcare/solutions/customer-service-solutions

**Xehetasuna:**

Kaltetutako produktuei eragiten dieten ahultasunak ondokoak dira:

- Memoriaren buffer baten mugetan eragiketen murrizketa desegokia. Horrek eragin lezake beste aldagai, datu egitura edo programaren barneko datu batzuei lotutako memoriaren kokapenetan egitea irakurketa eta idazketa eragiketak. Ondorioz, kode arbitrarioa exekuta liteke, aurreikusitako kontrolaren fluxua aldatu, informazio konfidentziala irakurri edo sistema ustekabean itxi.
- Garapenaz geroztik edo hirugarrenen osagaiak integratuz geroztik kodean/iturburu kodean dauden hainbat ahultasun.
- Informazioaren agerpena. Hori baliatuz erasotzaile batek informazio konfidentziala irakur edo zabal lezake baimenik gabe.
- Kode sorreraren (kode injekzioa) kontrol desegoki erako ahultasuna. Hori baliatuz jarraibide edo kode ez-baimenduak exekuta litezke.
- OWASPen top ten zerrendako ahultasunak. Horiek baliatuz baimendu gabeko baliabideetara sarbidea lor liteke edo jarraibide edo kode ez-baimenduak exekuta litezke.
- Modu desegokian murriztutako XML analizatzailea. Hori baliatuz sistemak fitxategi lokal bat irakur lezake eta erasotzaileak sarbide egokirik ez duen zerbitzarietara eskaerak bidal litzake.
- Hirugarrenen osagaietan ahultasunak. Hainbat eragin izan lezakete: zerbitzuaren ukapena, kode arbitrarioaren exekuzioa, sareko paketeen injekzioa, informazio konfidentziala eskuratzea edota baimendu gabeko pribilegioak eskuratzea. Horrela sistemaren konfidentzialtasuna, integritatea edo eskuragarritasuna kaltetu litezke.

**Etiketak:** Pribatutasuna, Ahultasuna

## Hainbat ahultasun Siemens-en Building

# Technologies produktuetan

**Argitalpen data:** 2018/04/02

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- License Management System (LMS), V2.1 SP3 (2.1.670) baino lehenagoko bertsio guztiak.
- Annual Shading V1.0.4 eta V1.1.
- Desigo ABT MP1.1 Build 845, MP1.15 Build 360, MP1.16 Build 055, MP1.2 Build 850, MP1.2.1 Build 318, eta MP2.1 Build 965.
- Desigo CC MP1.1, MP2.0, MP2.1, eta MP3.0.
- Desigo Configuration Manager (DCM) V6.10.140.
- Desigo XWP V5.00.204, V5.00.260, V5.10.142, V5.10.212, V6.00.184, V6.00.342 eta V6.10.172.
- SiteIQ Analytics V1.1, V1.2 eta V1.3.
- Siveillance Identity V1.1.

**Azalpena:**

Siemensek segurtasun buletin bat argitaratu du 8 ahultasunekin, horietatik 4 kritikoak eta 3 altuak. Horiek baliatuz kaltetutako gailuetan erasotzaile batek kode arbitrarioa exekuta lezake edo zerbitzuaren ukapen egoera sortu.

**Konponbidea:**

Siemensek erabiltzaileei aholkatzen die, beren ordezkariarekin edo bezeroaren arreta zerbitzuarekin harremanetan jarrita, kaltetutako produktuen bertsioak eguneratzea:

- LMS V2.1 SP4 (2.1.681) edo goragoko bertsioa instalatzea.

**Xehetasuna:**

- Gaizki sortutako ASN1 eskaerek sortutako larritasun kritikoko ahultasuna. Pilan oinarritutako bufferraren gainezkatzea eragin lezakete eta kode arbitrarioaren exekuzioa ahalbidetu. Ahultasun horretarako CVE-2017-11496 identifikatzailea erreserbatu da.
- Hizkuntzen paketean gaizki osatutako fitxategi izenek sortutako larritasun kritikoko ahultasuna. Pilan oinarritutako bufferraren gainezkatzea eragin lezakete eta kode arbitrarioaren exekuzioa ahalbidetu. Ahultasun horretarako CVE-2017-11497 identifikatzailea erreserbatu da.
- Larritasun kritikoko ahultasuna. NTLM-relay erasoak eragin ditzake, hizkuntzen paketea urrunetik manipulatuz. Ahultasun horretarako CVE-2017-12819 identifikatzailea erreserbatu da.
- Memoriaren hondatzeak sortutako larritasun kritikoko ahultasuna. Kodearen urruneko exekuzioa ahalbidetu lezake. Ahultasun horretarako CVE-2017-12821 identifikatzailea erreserbatu da.
- Hizkuntzen pakete trinkotuen HTML fitxategiek sortutako larritasun altuko ahultasuna. NULL erakuslerako sarbidea ahalbidetu lezakete, urruneko zerbitzu ukapen egoera eraginez. Ahultasun horretarako CVE-2017-11498 identifikatzailea erreserbatu da.
- XML analizatzailean pilan oinarritutako bufferraren gainezkatzeak sortutako larritasun altuko ahultasuna. Urruneko zerbitzu ukapen egoera eragin dezake. Ahultasun horretarako CVE-2017-12818 identifikatzailea erreserbatu da.
- Erakusletik memoriaren irakurketa arbitrarioak sortutako larritasun altuko ahultasuna. Urruneko zerbitzu ukapen egoera eragin dezake. Ahultasun horretarako CVE-2017-12820 identifikatzailea erreserbatu da.

**Etiketak:** Eguneraketa, Siemens, Ahultasuna

---

# Zerbitzuaren ukapena WAGO PLCetan

**Argitalpen data:** 2018/04/02

**Garrantzia:** Ertaina

**Kaltetutako baliabideak:**

Firmwarearen 10. bertsioa edo lehenagokoa duten WAGO  PLCen 750 serieko produktu hauek kaltetuta daude:

- 750-880
- 750-881
- 750-852
- 750-882
- 750-885
- 750-831
- 750-889
- 750-829

**Azalpena:**

Argitaratu den ahultasun bat baliatuz, erasotzaile batek zerbitzuaren ukapen egoera eragin lezake kaltetutako produktuetan.

**Konponbidea:**

WAGOk firmwarearen bertsio berriak argitaratu ditu, ohartarazpen honetan azaltzen den ahultasuna konpontzen dutenak. Firmwarearen bertsio berriak eskuratzeko WAGOrekin harremanetan jarri beharra dago ondoko helbide elektronikoan: [email protected].

**Xehetasuna:**

TCP komunikazio batek berezkoa duen hiru faseko hasierako negoziazioaren inplementazio oker batengatik, urruneko erasotzaile batek komunikazioak kaltetu litzake komisio eta zerbitzu tresnekin. Era berean, bereziki diseinatutako paketeak bidaliz 2455 TCP/IP atakara (Codesys kudeaketa softwareak erabilia), komunikazioetan zerbitzuaren ukapen egoera eragin liteke, aipatutako komisio eta zerbitzu tresnekin.

**Etiketak:** Eguneraketa, Komunikazioak, Ahultasuna

---

# Hainbat ahultasun MicroLogix 1400 gailuetan

**Argitalpen data:** 2018/04/02

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- Allen-Bradley Micrologix 1400 Series B FRN 21.003
- Allen-Bradley Micrologix 1400 Series B FRN 21.002
- Allen-Bradley Micrologix 1400 Series B FRN 21.0
- Allen-Bradley Micrologix 1400 Series B FRN 15

**Azalpena:**

Cisco Taloseko Jared Rittle eta Patrick DeSantis ikertzaileek Rockwell produktuei eragiten dieten hainbat ahultasunen berri eman dute. Horien ondorioz zerbitzuaren ukapena, informazio konfidentzialaren zabalkundea, komunikazioaren galera edota konfigurazioaren edo eskala logikoaren aldaketa eragin litezke.

**Konponbidea:**

Kaltetutako gailuen firmwarea ondoko bertsiora eguneratzea gomendatzen da:

- Allen-Bradley Micrologix 1400 FRN 21.004

Micrologix 1400 Series Aren edo Micrologix 1100en erabiltzaileei gomendatzen zaie Micrologix 1400 Series B edo Cra migratzea eta horretarako Rockwell Automationek aholkatzen du nor bere banatzailearekin harremanetan jartzea. Ahultasun honi buruzko informazio gehiago Rockwell Automationen orrian aurki daiteke.

Horrez gain, erabiltzaile kaltetuei gomendatzen zaie "keyswitch" giltzaren balioa "Hard Run" aukeran kokatzea, baimendu gabeko edozein aldaketa saihestearren.

Era berean, ahultasun horiek baliatuko lituzketen erasoak antzematearren, Cisco Talosek SNORTerako segurtasun arauak sortu ditu, ondoko identifikatzaileekin (SID): 44424, 44425, 44426, 44427, 44428 eta 44429.

**Xehetasuna:**

Cisco Taloseko ikertzaileek aurkitutako ahultasunak ondokoak dira:

- Zerbitzuaren ukapen erako ahultasuna Ethernet txarteleko gaizki sortutako pakete batengatik: ahultasun hau baliatuz erasotzaile batek gailuaren potentzia zikloa alda lezake eta bere huts egitea lortu. Ahultasun hau baliatzeko, gainera, ez da beharrezkoa Ethernet/IP erabiltzea, eta hortaz, RSLogix erabiliz hura desgaitzea ez litzateke aski izango. Ahultasun horretarako CVE-2017-12088 identifikatzailea erabili da.
- Zerbitzuaren ukapen erako ahultasuna deskargaren funtzionaltasuna erabiliz: Autentifikatu gabeko urruneko erasotzaile batek bereziki diseinatutako pakete bat bidal lezake kontrolatzailera, deskarga prozesu estandarra gertatzen ari denean. Deskargaren amaiera adierazteko pakete egokirik gabe, kontrolatzaileak huts egiten du. Ahultasun horretarako CVE-2017-12089 identifikatzailea erabili da.
- Zerbitzuaren ukapen erako ahultasuna SNMP ezartzeko eskari batekin: bereziki diseinatutako SNMP konfigurazioaren eskaera batek, firmwarearen parametroak aldatzeko balio egokirik gabe bidaltzen denean, gailua itzaltzea eta zerbitzuaren ukapen egoera eragin litzake. Ahultasun horretarako CVE-2017-12090 identifikatzailea erabili da.
- Gailura sartzeko kontrolean ahultasuna: Autentifikatu gabeko urruneko erasotzaile batek bereziki diseinatutako pakete bat bidal lezake kaltetutako gailura eta irakurketa edo idazketa eragiketak erabili. Horien bidez hainbat kalte eragin litzake, besteak beste: informazio konfidentzialaren zabalkundea, konfigurazioen aldaketa edo programaren logikaren aldaketa. Ahultasun honetarako CVE-2017-14462tik CVE-2017-14473ra bitarteko identifikatzaileak erabili dira, kaltetutako parametro edo fitxategiaren baitan.
- Memoriaren moduluan fitxategien idazketa ahultasuna: MicroLogix kontrolatzaile batean instalatutako memoria modulua baliatuz erabiltzaileak kontrolatzaileari erakuts diezaioke bere programa moduluan idatz dezan autentifikaziorik gabe. Memoria modulua segurtasun kopia bat da baina, era berean, programak kargatzeko ere erabil daiteke akats bat gertatzen denean, eta programa kargatzeko ahalmena du gailua pizten den bakoitzean. Ahultasun horretarako CVE-2017-12092 identifikatzailea erabili da.
- Saio gaiztoaren erregistro edo komunikazioen galera ahultasuna: MicroLogix 1400 kontrolatzaileak hamar saio aktibo onartzen ditu batera. Aurkitutako ahultasuna baliatuz asmo gaiztoko erabiltzaile batek bere saio paketeak bidal litzake kontrolatzailearekin bere konexio propioa sortzeko, erabiltzaile baliagarriak PLCra sar daitezen eragotziz. Horrez gain, hamar konexio daudenean, berri bat bidaltzerakoan zaharrena deskonektatu egiten da, komunikazioa etenda. Ahultasun horretarako CVE-2017-12093 identifikatzailea erabili da.

**Etiketak:** Eguneraketa, SCADA, Ahultasuna

---

# Ahultasuna Moxa-ren AWK-3131A-n

**Argitalpen data:** 2018/04/04

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- Moxa AWK-3131A Industrial IEEE 802.11a/b/g/n wireless AP/bridge/client, 1.7 eta lehenagoko bertsioak.

**Azalpena:**

Cisco Taloseko Patrick DeSantis eta Dave McDaniel ikertzaileek larritasun kritikoko ahultasun bat aurkitu dute Moxaren hari gabeko sare industrialeko AWK-3131A gailuetan. Ahultasun hori baliatuz autentifikaziorik gabeko urruneko erasotzaile batek administrazio eta komandoen exekuzio pribilegioak eskura litzake sistema eragilean.

**Konponbidea:**

Moxa fabrikatzaileak erabiltzaileen eskura jarri du ahultasuna konpontzen duen firmwarearen eguneraketa bat. Eguneraketa hori ondoko loturan eskura daiteke:

- Firmware para AWK-3131A versión 1.10

**Xehetasuna:**

Aurkitutako ahultasunaren arrazoia da saio hasiera akastunen kudeaketa oker bat. Hori baliatuz autentifikaziorik gabeko urruneko erasotzaile batek kodea injekta lezake zerbitzu ezberdinen saio hasierako eremuaren bidez (SSH, Telnet, komandoen kontsola). Horri esker erasotzaileak komandoak exekuta litzake sistema eragilean administrazio pribilegioekin. Ahultasun horretarako CVE-2017-14459 identifikatzailea erreserbatu da.

**Etiketak:** Eguneraketa, Ahultasuna

# Moxa MXview-ren web zerbitzariaren pasahitz pribatura sarbidea

**Argitalpen data:** 2018/04/06

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- MXview, 2.8 bertsioa eta lehenagokoak

**Azalpena:**

Ikerkuntza Digitalerako Leahy Zentroko Michael DePlante ikertzaileak jakinarazi duenez, Moxa MXviewren web zerbitzariak duen ahultasun bat baliatuz urruneko erasotzaile batek zerbitzariko pasahitz pribatu kriptografikoetara sarbidea lor lezake eta haiek irakurri.

**Konponbidea:**

- Moxak bere webean argitaratu du ahultasun hori konpontzen duen MXViewren 2.9 bertsioa.

**Xehetasuna:**

Aurkitutako ahultasuna baliatuz, HTTP GET eskaera baten bidez web zerbitzariko pasahitz pribatura sarbidea lor liteke eta hori irakurri. Horri esker, web zerbitzarira bidalitako informazioa deszifra lezake urruneko erasotzaile batek. Ahultasun horretarako CVE-2018-7506 identifikatzailea erabili da.

**Etiketak:** Eguneraketa, SCADA

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

**Argitalpen data:** 2018/04/09

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- U.motion Builder Software, 1.3.4 bertsioa eta lehenagokoak

**Azalpena:**

Zero-Day Initiativeko Rgod eta Constantin-Cosmin Craciun ikertzaileek Schneider Electricen U.motion Builder softwareari eragiten dioten hainbat ahultasun aurkitu dituzte. Erasotzaile batek kodea urrunetik exekuta lezake eta datuak baimenik gabe zabal litzake.

**Konponbidea:**

Schneider Electricek ahultasun horiek konpontzen dituen partxe bat argitaratu du. Partxea hemen eskura daiteke:

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

Era berean, Schneider Electricek ondoko segurtasunezko prebentzio neurriak eta praktika onak jarraitzea aholkatzen du:

- U.motion Builder exekutatzen duen makinaren aurrean suebaki bat izatea, sarbiderako kontrol arau zorrotzekin.
- Makina hori ez da zuzenean konektatu behar Internetera.
- Makina hori ez da DMZ batean kokatu behar.
- Ez da ahalbidetu behar trafikorik zuzenean Internetetik makinarantz.
- Makina horren barruan U.motion Systemen aurkako urruneko sarbidea beti egin behar da VPN konexio seguru baten bidez.
- U.motion Builder softwarerako konexioak mugatzea, benetako beharra duten konfiantzako makinek soilik egin dezaten.
- Makinaren beraren barnean U.builder Software aplikazioa nork exekuta dezakeen finkatzeko zerrenda zuriak erabiltzea.
- Windowsen suebakiak berak jatorriz eskaintzen dituen sarbiderako kontrolak erabiltzea.

**Xehetasuna:**

Ondoren zehazten dira larritasun altu edo kritikoak diren ahultasunak:

- Kodea urrutitik exekutatzea ahalbidetzen duen SQL injekzioa: "object_id" sarbide parametroak SQL injekzioa jasan dezake track_getdata.php fitxategiaren barnean. Ahultasun hori baliatuz erasotzaile batek kode arbitrarioa exekuta lezake. Larritasun altuko ahultasun horretarako CVE-2018-7765 identifikatzailea erabili da.
- Kodearen urruneko exekuzioa: update_module.php fitxategiko "update_file" parametroak ez dauka erabilera egokia. Autentifikatutako urruneko erasotzaile batek ahultasun hori balia lezake, zerbitzarira bereziki prestatutako eskaerak bidaliz. Larritasun altuko ahultasun horretarako CVE-2018-7777 identifikatzailea erabili da.
- Samba Cry: Bezero gaiztoek smbd zerbitzariko karpeta partekatura liburutegi bat igo lezakete idazketa baimenekin, eta zerbitzariak exekutatzea eragin lezakete. Larritasun kritikoko ahultasun horretarako CVE-2017-7494 identifikatzailea erabili da.

Larritasun ertaineko gainerako ahultasunetarako erreserbatu diren kodeak honakoak dira: CVE-2018-7763, CVE-2018-7764, CVE-2018-7766, CVE-2018-7767, CVE-2018-7768, CVE-2018-7769, CVE-2018-7770, CVE-2018-7771, CVE-2018-7772, CVE-2018-7773, CVE-2018-7774, CVE-2018-7775, CVE-2018-7776 .

**Etiketak:** Eguneraketa, PHP, Schneider Electric, Ahultasuna

# Hainbat ahultasun Omron-en CX-One softwarean

**Argitalpen data:** 2018/04/11

**Garrantzia:** Ertaina

**Kaltetutako baliabideak:**

- CX-One, 4.42 bertsioa eta lehenagokoak, ondoko aplikazioak barne:
  - CX-FLnet, 1.00 bertsioa eta lehenagokoak
  - CX-Protocol, 1.992 bertsioa eta lehenagokoak
  - CX-Programmer, 9.65 bertsioa eta lehenagokoak
  - CX-Server, 5.0.22 bertsioa eta lehenagokoak
  - Network Configurator, 3.63 bertsioa eta lehenagokoak
  - Switch Box Utility, 1.68 bertsioa eta lehenagokoak

**Azalpena:**

Trend Microko Zero Day Initiativeko Rgod ikertzaileak Omron-en CX-One softwareari eragiten dioten hainbat ahultasun aurkitu ditu, bi ahultasun bufferraren gainezkatze erakoak eta beste bat mota bateraezineko baliabideetarako sarbide erakoa. Erasotzaile batek kodea urrunetik exekutatzea lor lezake.

**Konponbidea:**

Omronek kaltetutako produktuen bertsio berriak argitaratu ditu, honakoak hain zuzen:

- X-FLnet, 1.10 bertsioa
- CX-Protocol, 1.993 bertsioa
- CX-Programmer, 9.66 bertsioa
- Common Module, CX-Server barne duena, 5.0.23 bertsioa
- Network Configurator, 3.64 bertsioa
- Switch Box Utility, 1.69 bertsioa

**Xehetasuna:**

- Pilak gainezka egitea: Gaizki sortutako proiektu fitxategien tratamenduak bufferraren gainezkatzea eragin dezake eta horrek stack-a eta heap-a kaltetu ditzake. Ahultasun horretarako CVE-2018-8834 eta CVE-2018-7514 kodeak erabili dira.
- Mota bateraezineko baliabideetarako sarbidea: Gaizki sortutako proiektu fitxategien tratamendua baliatuz, erakusleak objektu okerra dei lezake, eta ondorioz baliabide baterako sarbidea gerta liteke bateragarria ez den baldintza mota bat erabiliz. CVE-2018-7530 kodea esleitu zaio ahultasun horri.

**Etiketak:** Ahultasuna

---

# Hainbat ahultasun ATI Systems-en larrialdien jakinarazpen masiboen sistemetan

**Argitalpen data:** 2018/04/11

**Garrantzia:** Ertaina

**Kaltetutako baliabideak:**

- HPSS16
- HPSS32
- MHPSS
- ALERT4000

**Azalpena:**

Bastilleko Balint Seeber-ek autentifikazio ezegokiaren eta zifratze gabeziaren erako bi ahultasunen berri eman du, ATI Systems-en larrialdien jakinarazpen masiboko zenbait gailuri eragiten dietenak. Erasotzaile batek alarma faltsuak eragin litzake.

**Konponbidea:**

ATI Systemsek partxe bat sortu du, irrati bitartez bidalitako paketeei segurtasun funtzionalitate berriak gehitzen dizkiena. ATI Systems partxea probatzen ari da eta eskariei erantzunez banatuko da. Horrez gain, sistema asko erabiltzaileentzat bereziki diseinatuta daudela adierazi du eta erabiltzaileak berak arduratu behar dutela euren sistementzat eguneraketak egokiak diren ziurtatzeaz.

ATI Systemsek aholkatzen du posible denean ahots soileko irrati sistemak aldatzea P-25 (APCO) irrati sistema digitalengatik, lotura zifratu seguruak eskaintzen baitituzte.

**Xehetasuna:**

- Autentifikazio okerra: Bereziki gaizki sortutako irrati pakete bat baliatuz erasotzaile batek alarma faltsuak bidal litzake urrunetik. Ahultasun horretarako CVE-2018-8862 identifikatzailea erreserbatu da.
- Datu sentikorren zifratze falta: Bereziki gaizki sortutako irrati pakete bat baliatuz erasotzaile batek alarma faltsuak bidal litzake urrunetik. Ahultasun horretarako CVE-2018-8864 identifikatzailea erreserbatu da.

**Etiketak:** Komunikazioak, Pribatutasuna, Ahultasuna

---

# Sarbidearen kontrol erako ahultasuna Yokogawa-ren CENTUM eta Exaopc-en

**Argitalpen data:** 2018/04/13

**Garrantzia:** Ertaina

**Kaltetutako baliabideak:**

- CENTUM series
  - CENTUM CS 1000ren bertsio guztiak
  - CENTUM CS 3000, R3.09.50 eta lehenagoko bertsioak
  - CENTUM CS 3000 Small, R3.09.50 eta lehenagoko bertsioak
  - CENTUM VP, R6.03.10 eta lehenagoko bertsioak
  - CENTUM VP Small, R6.03.10 eta lehenagoko bertsioak
  - CENTUM VP Basic, R6.03.10 eta lehenagoko bertsioak
- Exaopc, R3.75.00 eta lehenagoko bertsioak
- B/M9000 CS bertsio guztiak
- B/M9000 VP, R8.01.01 eta lehenagoko bertsioak

**Azalpena:**

Yokogawa enpresak, JPCERTekin lankidetzan, Yokogawaren CENTUM eta Exaopc-en baimenetan, pribilegioetan eta sarbide kontroletan dauden ahultasunen berri eman du. Erasotzaile batek prozesuaren edo sistemaren alarma faltsuak eragin litzake eta sistema blokea lezake bai eta alarmak ikusteko prozesuak ere.

**Konponbidea:**

Kaltetutako produktuetarako hainbat arintze argitaratu ditu Yokogawak.

- CENTUM series
  - CENTUM CS 1000, CENTUM CS 3000, CENTUM CS 3000 Small: Ez da eguneraketarik eskainiko gailu horiek zerbitzuz kanpo daudelako. Fabrikatzaileak gomendatzen du gailua CENTUM VPren azken bertsioagatik aldatzea.
  - CENTUM VP, CENTUM VP Small, CENTUM VP BASIC: Kaltetutako erabiltzaileek gailu horiek egunera ditzakete R5.04.B2 edo R6.04.00 bertsioetara.
- Exaopc: kaltetutako erabiltzaileek sistema R3.76.00 bertsiora eguneratu behar lukete.
- B/M9000CS: produktu honek ez du ahultasunik. Nolanahi ere, PC berean ahultasuna eragiten dion softwarerik badago, gailuaren alarmei eragin diezaieke
- B/M9000 VP: produktu honek ez du ahultasunik. Nolanahi ere, PC berean ahultasuna eragiten dion softwarerik badago, gailuaren alarmei eragin diezaieke

**Xehetasuna:**

Sarbide kontrolak duen ahultasun bat baliatuz, erasotzaile batek lokalki balia lezake sistemaren mezuen kudeaketarekin zerikusia duen funtzio bat. Ahultasun horretarako CVE-2018-8838 identifikatzailea erreserbatu da.

**Etiketak:** Eguneraketa, Ahultasuna

---

# Hainbat ahultasun Moxa-ren EDR-810 router industrialean

**Argitalpen data:** 2018/04/16

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- Moxa EDR-810 V4.1 build 17030317 eta agian aurreko bertsioak ere bai

**Azalpena:**

Cisco Taloseko Carlos Pacho ikertzaileak hainbat ahultasun aurkitu ditu Moxa EDR-810 router industrialean. Ahultasun horiek gailuak duen web zerbitzariari eragiten diote batez ere eta, besteak beste, erasotzaile batek ondoko ekintzak egin litzake: pribilegioen igoera komandoen injekzioaren bitartez, informazioaren zabalkundea baimenik gabe (gailuaren pasahitzak barne), konfigurazioan aldaketak CSRF bidez edo zerbitzuaren ukapen egoera sortzea kaltetutako produktuetan.

**Konponbidea:**

Fabrikatzaileak firmwarearen eguneraketa bat argitaratu du, gailuari eragiten dioten ahultasun guztiak konpontzen dituena.

Eguneraketa hori ondoko loturatik deskarga daiteke:

https://www.moxa.com/support/download.aspx?type=support&id=15851

**Xehetasuna:**

Ondoren zehazten dira larritasun altuko ahultasunak:

- Komandoen injekzioa: erasotzaile batek bereziki diseinatutako POST eskari bat bidal lezake gailuaren web zerbitzarira, sisteman pribilegioen eskalatzea lortzearren. Erasotzaile batek ahultasun hau balia lezake Sistema Eragilearen komandoak injektatuz "*/goform/net_WebPingGetValue*" URIaren ip parametroan. Ahultasun horretarako CVE-2017-12120 identifikatzailea erabili da.
- CSRF: Cross-Site Request Forgery erako ahultasuna dauka Moxa EDR-810 V4.1ren Web zerbitzariak. Erasotzaile batek CSRF erako ahultasun hori balia lezake, bereziki diseinatutako HTTP pakete bat bidaliz. Erasotzaileak pakete hori baliatuko luke gailua arriskuan jar dezaketen ekintzak egiteko. CVE-2017-12126 kodea esleitu zaio ahultasun horri.
- Komandoen injekzioa: Moxa EDR-810 V4.1en OpenVPN Web zerbitzariaren funtzionaltasunetako batek komandoen injekzioko ahultasun bat dauka. Erasotzaile batek ahultasun hori balia lezake HTTP pakete bat bidaliz bereziki diseinatutako POST metodoaren bidez. Pakete hori baliatuz erasotzaileak pribilegioen eskalatzea egin lezake, supererabiltzaile baten "shell" bat lortuz pribilegio gorenekin. Erasotzaile batek ahultasun hau balia lezake Sistema Eragilearen komandoak injektatuz "/goform/net_Web_get_value" URIaren parametroetan. Ahultasun horietarako CVE-2017-14432 eta CVE-2017-14434 erabili dira.
- Komandoen injekzioa: erasotzaile batek bereziki diseinatutako POST eskari bat bidal lezake gailuaren web zerbitzarira, sisteman pribilegioen eskalatzea lortzearren. Eskaera hori baliatuz erasotzaileak pribilegioen eskalatzea egin lezake, supererabiltzaile baten "shell" bat lortuz pribilegio gorenekin. Erasotzaile batek ahultasun hau balia lezake Sistema Eragilearen komandoak injektatuz "*/goform/WebRSAKEYGen*" URIaren rsakey_name parametroan. Ahultasun horretarako CVE-2017-12121 identifikatzailea erabili da.

- Komandoen injekzioa: erasotzaile batek bereziki diseinatutako POST eskari bat bidal lezake gailuaren web zerbitzarira, sisteman pribilegioen eskalatzea lortzearren. Eskaera hori baliatuz erasotzaileak pribilegioen eskalatzea egin lezake, supererabiltzaile baten "shell" bat lortuz pribilegio gorenekin. Erasotzaile batek ahultasun hau balia lezake Sistema Eragilearen komandoak injektatuz "*/goform/net_WebCSRGen*" URIaren CN parametroan. Ahultasun horretarako CVE-2017-12125 identifikatzailea erabili da.

- "*Service Agent*" DoS erako hainbat ahultasunekin: Moxa EDR-810 (V4.1 build 17030317) gailuak duen "*Service Agent*" funtzionaltasunak DoS erako ahultasunak ditu. Bereziki diseinatutako pakete bat 4000/tcp edo 4001/tcp ataketara bidaliz gero, zerbitzuaren ukapen egoera sor liteke. Ahultasun horietarako CVE-2017-14438 eta CVE-2017-14439 identifikatzaileak erabili dira.

- Sarbide datuen balioztatze okerra: bereziki diseinatutako URI HTTP batek NULL erakuslearen deserreferentzia erako ahultasuna eragin lezake, eta ondorioz web zerbitzariaren akats bat eragin. Erasotzaile batek zerbitzuaren ukapena eragin lezake gaizki sortutako URI bat bidaliz. Ahultasun horretarako CVE-2017-12124 identifikatzailea erreserbatu da.

- Zerbitzuaren Ukapena Moxa EDR-810 V4.1en Web zerbitzariaren funtzionaltasunetako batean. Erasotzaile batek zerbitzuaren ukapena eragin lezake bereziki gaizki sortutako URI HTTP bat bidaliz. Eskaera horrek NULL erakuslearen gaizki kudeatutako deserreferentzia bat eragin lezake. GET metodoaren bidez eskaera bat bidaliz gero "/MOXA_LOG.ini, /MOXA_CFG.ini, or /MOXA_CFG2.ini"-ren aurka  cookie goibururik gabe, ahultasun hau gertatuko litzateke. Ahultasun horietarako CVE-2017-14435 eta CVE-2017-14437 erabili dira.

Larritasun ertain eta baxuko gainerako ahultasunetarako erreserbatu diren kodeak honakoak dira: CVE-2017-12123, CVE-2017-12128, CVE-2017-12127 eta CVE-2017-12129.

**Etiketak:** Eguneraketa, Ahultasuna

---

# Hainbat ahultasun Schneider Electric-en produktuetan

**Argitalpen data:** 2018/04/18

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- Schneider Electric-en Triconex Tricon, MP 3008 modeloa, firmwarearen 10.0-10.4 bertsioak
- InduSoft Web Studio v8.1 eta lehenagoko bertsioak
- InTouch Machine Edition 2017 v8.1 eta lehenagoko bertsioak

**Azalpena:**

Tenable Researchek bufferraren gainezkatze erako ahultasun baten berri eman zion Schneider Electric-i. Horrez gain, NCCICek eta Schneider Electric-ek beste bi ahultasun gehiago aurkitu dituzte HatMan malwarearen ikerkuntzan.

Ahultasun horiek baliatuko lituzkeen erasotzaile batek honako ekintzak egin litzake, besteak beste: kodearen exekuzio arbitrarioa, sistemak itzaltzea, babes sistemak arriskuan jartzea edo kaltetutako gailuak erabateko arriskuan jartzea.

**Konponbidea:**

- Indusoft Web Studio eta InTouch Machine Edition-en bufferraren gainezkatze erako ahultasunaren kasuan, fabrikatzaileak gomendatzen du eragindako produktuen kaltetutako bertsioak eguneratzea:
  - InduSoft Web Studio v8.1 edo lehenagoko bertsioak erabiltzen dituzten erabiltzaileek InduSoft Web Studio v8.1 SP1 bertsiora eguneratu beharko lukete ahalik azkarren. Hauxe da eguneraketa deskargatzeko lotura: http://download.indusoft.com/81.1.0/IWS81.1.0.zip
  - Machine Edition 2017 v8.1 edo lehenagoko bertsioak erabiltzen dituzten erabiltzaileek Machine Edition 2017 v8.1 SP1 bertsiora eguneratu beharko lukete ahalik eta azkarren. Hauxe da eguneraketa deskargatzeko lotura: https://fs-ext.invensys.com/adfs/ls/?wa=wsignin1.0&wtrealm=https://gcsresource.schneider-electric.com&wctx=rm=0&id=passive&ru=%2ftracking%2fConfirmDownload.aspx%3fid%3d22530&wct=2018-04-18T07:35:10Z
- Triconex Tricon gailuari eragiten dion ahultasunaren kasuan, fabrikatzaileak aholkatzen du firmwarea 11.X azken bertsiora eguneratzea, gailuari eragiten dioten ahultasun guztiak konpontzen dituena.

**Xehetasuna:**

Ondoren zehazten dira Schneider Electric-en Triconex Tricon-en MP 3008 modeloari eragiten dioten ahultasun guztiak:

- **Memoriaren gunean idazketa baimenen kudeaketa okerra:** Sistemaren deiek zuzenean irakurtzen dute memoriaren gunea, prozesuaren aldetik inolako kontrolik gabe eta inolako egiaztapenik gabe. Memoriako datuen manipulazioari esker, erasotzaile batek jarraibideak kopia litzake memoriaren edozein gunetan. Larritasun kritikoko ahultasun horretarako CVE-2018-8872 identifikatzailea erabili da.

- **Memoriaren gunean idazketa baimenen kudeaketa okerra:** Sistemara dei bat egiten denean, erregistroak kokapen finko batean gordetzen dira. Erasotzaile batek memoriaren gune finko horretako datuak alda ditzake eta sistemen egoeraren edo sistema gainbegiralearen kontrola hartu. Larritasun altuko ahultasun horretarako CVE-2018-7522 kodea erabili da.

Bestalde, Indusoft Web Studio eta InTouch Machine Edition produktuei eragiten dien ahultasunaren xehetasuna honakoa da:

- **Bufferrak gainezka egitea:** Urruneko erasotzaile batek gaizki sortutako pakete bat egin lezake alarma, etiketa edo ekintzetan irakurketa edo idazketa gertakariak ematen ari diren bitartean bidaltzeko. Horrela urruneko kodea pribilegio gorenekin exekutatzea lor lezake. Larritasun kritikoko ahultasun horretarako CVE-2018-8840 identifikatzailea erreserbatu da.

**Etiketak:** Eguneraketa, Schneider Electric, Ahultasuna

---

# Hainbat ahultasun Abbott Laboratories-en ICD eta CRT-D bihotz inplanteetan

**Argitalpen data:** 2018/04/18

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

Abbott Laboratories-en ICD (Implantable Cardioverter Defibrillator) eta CRT-Dren (Cardiac Synchronization Therapy Defibrillator) ondoko modeloak:

- Fortify
- Fortify Assura
- Quadra Assura
- Quadra Assura MP
- Unify
- Unify Assura
- Unify Quadra
- Promote Quadra
- Ellipse
- Current
- Promote

**Azalpena:**

MedSec Holdings Ltd.-k ahultasun hauen berri eman die NCCIC eta Abbott Laboratories-i. Gailutik gertu dagoen erasotzaile batek irrati frekuentziaren barrutian interferitu dezake, autentifikazioa saihestu eta baimenik gabe sarbidea lortu, komandoak aldatzeko, aldagaiak aldatzeko edo gailuaren funtzionamendu egokian eragiteko.

**Konponbidea:**

Fabrikatzaileak firmwarearen eguneraketa bat argitaratu du, bere produktuetan aurkitutako ahultasun guztiak konpontzen dituena. Eguneraketa hori Merlin PCS Programmer bitartez aplika dezake osasun arretaren hornitzaileak. Abbott-ek eta FDAk gomendatzen dute eguneraketa hori paziente guztiei jartzea programatuta duten hurrengo bisitan, edo egokitzat jotzen denean, pazientearen eta medikuaren nahien arabera. 2018ko apirilaren 25etik aurrera fabrikatutako ICD eta CRT-D guztiek eguneraketak aurrez instalaturik dituzte.

Aurrekoaz gain, Cybersecurity Medical Advisory Board-ek ondoko neurri prebentiboak gomendatzen ditu:

- Osasun arretako hornitzaileek eta pazienteek aztertu behar dituzte hurrengo bisitan ahultasun hauen arriskuak eta onurak eta dagokien firmwarearen eguneraketak. Kontuan hartu behar dira pazienteen kasu zehatzak, esate baterako: taupada markagailuarekiko mendekotasuna, tentsio garaiko terapiaren maiztasuna, gailuaren adina eta pazientearen nahia. Era berean, pazienteei "Pazientearekiko komunikazioa" eman behar zaie.
- Erabaki behar da ea firmwarearen eguneraketa egokia den, pazienteak eguneraketarako duen arriskuaren baitan. Egokitzat jotzen bada, fabrikatzaileak emandako jarraibideen arabera instalatu behar da firmwarearen eguneraketa.
- Firmwarearen eguneraketa egin behar da monitorizazioko eta kanpo desfibrilazioko sistema egokiak dituen instalazio batean.

**Xehetasuna:**

- Egiaztatze okerra: Autentifikaziorako erabiltzen den algoritmoa, autentifikazio pasahitza eta denbora balioa erabiltzen dituena, arriskutan jarria edo saihestua izan daiteke. Hori baliatuz, gertuan dagoen erasotzaile batek komandoak bidal litzake ICD edo CRT-D gailuetara irrati frekuentziaren seinaleak aldatuz. Larritasun altuko ahultasun horretarako CVE-2017-12712 kodea erabili da.
- Bateriaren kontsumoari eragiten dioten eskaerei buruzko murrizpen okerrak: Egin daitezkeen 'RF wake-up' erako eskaeren kopurua ez dute modu egokian kudeatzen ICD edo CRT-D gailuek. Hori baliatuz, gertuan dagoen erasotzaile batek horrelako komando mota pila bat bidal litzake, bateriaren bizitza erabilgarria murriztearren. Larritasun ertaineko ahultasun horretarako CVE-2017-12714 kodea erabili da.

**Etiketak:** Eguneraketa, Ahultasuna

---

# Hainbat ahultasun Biosense Webster-en CARTO 3-n

**Argitalpen data:** 2018/04/18

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- CARTO 3 sistemak, 2018ko apirilaren 3a baino lehen fabrikatutakoak.

**Azalpena:**

CARTO 3 sistemari eragiten dioten ahultasunak baliatuz, gailura sarbide fisikoa lukeen erasotzaile batek gailuan bertan gordetako informazioa eskura lezake, pazienteen osasun informazioa barne. Horrek CARTO 3 sistemaren integritateari eragingo lioke eta zerbitzuaren ukapen egoera sor lezake.

**Konponbidea:**

Biosense Webster kaltetutako bezeroekin harremanetan jartzen ari da, ahultasunak arintzen dituen eguneraketa prozesua abiatzearren.

Biosense Webster-ek gomendatzen du CARTO 3 familiako edozein produkturako sarbide fisikoa murriztea, segurtasun partxea jaso bitartean.

**Xehetasuna:**

CARTO 3 V4 sistemara sarbide fisikoa eta ahultasunen ezagupena lukeen erasotzaile batek horietako batzuk balia litzake gailuaren informazioa arriskuan jarriz, bai eta integritateari eta sistemaren eskuragarritasunari eraginez.

Ahultasunen zerrenda osoaren xehetasunak ezagutzeko irakurri Biosense Webster-en ohar ofiziala.

**Etiketak:** Ahultasuna

---

# Hainbat ahultasun ABBren Relion 630 series-en

**Argitalpen data:** 2018/04/18

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- Relion® 630 series 1.1
- Relion® 630 series 1.2
- Relion® 630 series 1.3
- Relion® 630 series 1.1, 1.1.0.C1 eta lehenagokoak.
- Relion® 630 series 1.2, 1.2.0.B4 eta lehenagokoak.
- Relion® 630 series 1.3, 1.3.0.A7 eta lehenagokoak.

**Azalpena:**

Aleksandr Tlyapov (Kaspersky Lab), Kirill Nesterov (Kaspersky Lab), Ilya Karpov, Evgeniy Druzhinin, Damir Zainullin (Positive Technologies) eta Victor Nikitin (i-Grids) ikertzaileek hainbat ahultasun aurkitu dituzte. Horiek baliatuz, erasotzaile batek ondoko ekintzak egin litzake: gailuaren zerbitzuaren ukapen egoera eragin lezakeen datu basearen ezabaketa/aldaketa, flash memoriaren edozein fitxategiren irakurketa eta aldaketa autentifikaziorik gabe, gailuan zerbitzuaren ukapen egoera eragin lezakeena edo kaltetutako produktuetan beste zerbitzuaren ukapen egoera bat eragin lezakeena.

**Konponbidea:**

Ohartarazpen honetan azaldutako ahultasunak, larritasun ertainekoa den datu basearen zifratu ahularena salbu, konpontzen dituzten firmware bertsioak daude.

Ondoko loturetan ikus daitezke azaldutako ahultasunak konpontzen dituzten firmware bertsioak:

http://search.abb.com/library/Download.aspx?DocumentID=1MRS758877&LanguageCode=en&DocumentPartId=&Action=Launch

http://search.abb.com/library/Download.aspx?DocumentID=1MRS758878&LanguageCode=en&DocumentPartId=&Action=Launch

http://search.abb.com/library/Download.aspx?DocumentID=1MRS758909&LanguageCode=en&DocumentPartId=&Action=Launch

**Xehetasuna:**

Ondoren zehazten dira ABBren Relion 630 series gailuei eragiten dieten ahultasunak:

- Fitxategien bideen kudeaketa okerra: Kaltetutako gailuetan barneratutako MMS zerbitzariak duen ahultasun bat baliatuz, erasotzaile batek bereziki gaizki sortutako eskaerak bidal litzake, fitxategien bideetara sarbidea lortzeko COMTRADE direktorioaren mugez kanpo, fopen eta fdelete komandoak baliatuz. Horrek edozein bidetan fitxategiak irakurtzea/idaztea ahalbidetu lezake, funtzio horretarako zehaztutako direktorioaren muga saihestuz. Ahultasun honek soilik eragiten die IEC 61850 MMS protokoloa gaituta duten gailuei.
- Datu basearen enkriptatze pasahitzak sortzerakoan ahultasuna: erasotzaile batek ahultasun hori balia lezake datu basea aldatzeko, eta aldaketa horien eraginez Zerbitzuaren Ukapen egoera sor liteke.
- Komandoen maneiatzailean ahultasuna: erasotzaile batek ahultasun hau balia lezake gaizki sortutako paketeak bidaltzeko. Horrek gailuaren nahitaezko berrabiatzea eragingo luke. Berrabiatze fasean gailuaren babeserako funtzionaltasun nagusia ez litzateke eskuragarri egongo.

**Etiketak:** Eguneraketa, Ahultasuna

---

# Hainbat ahultasun Rockwell Automation-en produktuetan

**Argitalpen data:** 2018/04/18

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

Cisco IOS edo IOX XEren bertsio kaltetuak dituzten gailuak:

- Kudeatutako Ethernet Allen-Bradley Stratix 8300 Industrial switchak, 15.2(4a)EA5 bertsioa eta lehenagokoak.
- Allen-Bradley Stratix 5400 Industrial switchak, 15.2(6)E0a bertsioa eta lehenagokoak.
- Allen-Bradley Stratix 5410 Industrial Distribution switchak, 15.2(6)E0a bertsioa eta lehenagokoak.
- Kudeatutako Ethernet Allen-Bradley Stratix 5700 Industrial switchak, 15.2(6)E0a bertsioa eta lehenagokoak.
- Kudeatutako Ethernet Allen-Bradley Stratix 8000 Modular switchak, 15.2(6)E0a bertsioa eta lehenagokoak.
- Muturreko inguruneetarako kudeatutako Allen-Bradley ArmorStratix 5700 Industrial switch industrialak, 15.2(6)E0a eta lehenagoko bertsioak.
- Allen-Bradley Stratix 5900 Services routerrak, 15.6.3M1 bertsioa eta lehenagokoak.

**Azalpena:**

Rockwell Automationek ahultasun horien berri eman dio NCCICi "Cisco IOS and IOS XE Software Security Advisory Bundled Publication" izeneko sei hileroko argitalpenaren bidez. Urruneko erasotzaile batek ahultasun mota hauek balia litzake: sarrera parametro baliogabeak, akatsen kudeaketa okerra, bufferraren memoriaren mugen barneko eragiketen murrizketa okerra edo eskuragarritasunaren galera lortzeko kanpotik kontrolatutako kateen formatua, memoriako baliabideak agortzeagatik sortutako konfidentzialtasuna edota integritatea, komunikazio moduluen berrabiatzea, informazioaren hondamena edota informazioaren agerpena.

**Konponbidea:**

Ciscok Snort arauak argitaratu ditu ondoko loturan:

https://www.cisco.com/web/software/286271056/117258/sf-rules-2018-03-29-new.html

Arau horiek ondoko kodeetara lotutako ahultasunak arintzen dituzte:

- CVE-2018-0171 - 46096. eta 46097. Snort araua
- CVE-2018-0156 - 41725. Snort araua
- CVE-2018-0174 - 46120. Snort araua
- CVE-2018-0172 - 46104. Snort araua
- CVE-2018-0173 - 46119. Snort araua
- CVE-2018-0158 - 46110. Snort araua

Ciscok ondoko ohartarazpenak gehitu dizkie ahultasunei (**CVE-2018-0171 y CVE-2018-0156**):

- Smart Install funtzionaltasunaren konfigurazioa espresuki dator desgaituta. Nolanahi ere, switchen eguneraketak aukera hori gaitu lezake, ez ordea berriz instalatzeak.
- Smart Install funtzionaltasuna desgaitzea "no vstack" konfigurazio komandoarekin, beharrezkoa ez bada edo instalazioa egin ondoren.
- Smart Install funtzionaltasuna erabiltzen duten (eta desgaituta utzi beharra duten) erabiltzaileek ACLak erabil ditzakete 4786/tcp atakara sartzen den trafikoa blokeatzeko.

**CVE-2018-0155:** Beren inguruneetan BFD funtzionaltasuna erabiltzen ez duten administratzaileek funtzionaltasun hori desgai dezakete dagokion "bfd" komandoarekin, ahultasuna baliatu ahal izatea saihestearren.

Bestalde, funtzionaltasun hori erabiltzen duten administratzaileek kontrol politikak (CoPP) jar ditzakete abian, soilik BFD pakete ezagunen prozesamendua baimentzeko eta kaltetutako produktuaren arriskua mugatzeko.

CVE-2018-0167 eta CVE-2018-0175 kodeei lotutako ahultasunek ez daukate arintze modu berezirik. Informazio gehiagorako, fabrikatzailearen ondoko lotura bisitatzea gomendatzen da:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-lldp

Bestalde, Rockwell Automation fabrikatzaileak segurtasuneko ondoko neurri prebentiboak eta praktika onak jarraitzea gomendatzen du:

- Kontrol gailu edota sistema guztien arriskua murrizten laguntzearren, suebakien atzean kokatzea gomendatzen da, eta gailuek edota sistemek Interneterako sarbiderik ez dutela egiaztatzea.
- Kontrol sareak eta gailu industrialak sare korporatiboetatik bereiztea.

Urruneko sarbidea beharrezkoa denean, Virtual Private Networks (VPN) moduko segurtasun mekanismoak erabiltzea.

**Xehetasuna:**

- Sarrera datuen balioztatze ezegokia: Cisco IOS eta Cisco IOS XE Softwarearen Smart Install funtzionaltasunak duen ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek kaltetutako gailua berrabiatzea eragin lezake. Horren ondorioz kaltetutako gailuan zerbitzuaren ukapen egoera (DoS) sortuko litzateke edo kode arbitrarioa exekuta liteke. Ahultasunaren arrazoia da paketeko datuen egiaztapen okerra. Erasotzaile batek ahultasun hori balia lezake Smart Installen mezu pakete bat bidaliz TCP 4786 atakan kaltetutako gailu batera. Eraso arrakastatsu baten ondorioz erasotzaileak bufferraren gainezkatzea eragin lezake kaltetutako gailuan. Larritasun kritikoko ahultasun horretarako CVE-2018-0171 identifikatzailea erabili da.
- Sarrera datuen balioztatze ezegokia: Cisco IOS eta Cisco IOS XE Softwarearen Smart Install funtzionaltasunak duen ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek kaltetutako gailua berrabiatzea eragin lezake. Horren ondorioz kaltetutako gailuan zerbitzuaren ukapen egoera (DoS) sortuko litzateke. Ahultasunaren arrazoia da paketeko datuen egiaztapen okerra. Erasotzaile batek ahultasun hori balia lezake pakete bat bidaliz TCP 4786 atakan kaltetutako gailu batera. Larritasun kritikoko ahultasun horretarako CVE-2018-0156 identifikatzailea erabili da.
- Sarrera datuen balioztatze ezegokia: Cisco IOS eta Cisco IOS XE softwarearen DHCP enkapsulazio funtzionaltasunaren 82. aukerak duen ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek kaltetutako gailua berrabiatzea eragin lezake. Horren ondorioz zerbitzuaren ukapen egoera (DoS) sortuko litzateke. Ahultasun hau gertatzen da birtransmisio agenteen aldetik DHCP 4. Bertsioaren (DHCPv4) paketeetatik jasotzen duen sarreraren egiaztatze osatugabea egiten duelako kaltetutako softwareak. Erasotzaile batek ahultasun hori balia lezake DHCPv4 pakete bat bidaliz kaltetutako gailu batera. Eraso arrakastatsu bat izanez gero, erasotzaileak gailua berrabiatzea eragin lezake, eta horren ondorioz zerbitzuaren ukapen egoera sortu (DoS). Larritasun kritikoko ahultasun horretarako CVE-2018-0174 identifikatzailea erabili da.
- Sarrera datuen balioztatze ezegokia: Cisco IOS eta Cisco IOS XE softwarearen DHCP enkapsulazio funtzionaltasunaren 82. aukerak duen ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek kaltetutako gailua berrabiatzea eragin lezake. Horren ondorioz zerbitzuaren ukapen egoera (DoS) sortuko litzateke. Ahultasun hau gertatzen da birtransmisio agenteen aldetik DHCP 4. Bertsioaren (DHCPv4) paketeetatik jasotzen duen sarreraren egiaztatze osatugabea egiten duelako kaltetutako softwareak. Erasotzaile batek ahultasun hori balia lezake DHCPv4 pakete bat bidaliz kaltetutako gailu batera. Eraso arrakastatsu bat izanez gero, erasotzaileak heap-en gainezkatzea eragin lezake, eta horren ondorioz zerbitzuaren ukapen egoera sortu (DoS). Larritasun kritikoko ahultasun horretarako CVE-2018-0172 identifikatzailea erabili da.
- Sarrera datuen balioztatze ezegokia: Cisco IOS eta Cisco IOS XE softwareak duen ahultasun bat baliatuz, DHCP 4. Bertsioaren (DHCPv4) paketeen enkapsulazioaren 82. aukera berrezartzen duena, autentifikatu gabeko urruneko erasotzaile batek kaltetutako gailua berrabiatzea eragin lezake. Horren ondorioz zerbitzuaren ukapen egoera (DoS) sortuko litzateke. Ahultasun hau gertatzen da kaltetutako softwareak DCHPv4 zerbitzarietatik datozen DHCPOFFER mezuen 82. enkapsulazio aukeraren informazioarekin jasotzen duen sarreraren egiaztapen osagabea ezartzen duelako. Erasotzaile batek ahultasun hori balia lezake DHCPv4 pakete bat bidaliz kaltetutako gailura, ondoren gailu horrek DHCPv4 zerbitzari batera birbidal dezan. Zerbitzariaren erantzunean enkapsulaturik dagoen 82. aukerarekin prozesatzen duenean informazioa kaltetutako softwareak, akats bat gerta liteke. Eraso arrakastatsu bat izanez gero, erasotzaileak gailua berrabiatzea eragin lezake, eta horren ondorioz zerbitzuaren ukapen egoera sortu (DoS). Larritasun kritikoko ahultasun horretarako CVE-2018-0173 identifikatzailea erabili da.
- Sarrera datuen balioztatze ezegokia: Cisco IOs eta Cisco IOS XE softwareak Internet Key Exchange Versión 2 (IKEv2) moduluan duen ahultasun bat baliatuz, autentifikaziorik gabeko urruneko erasotzaile batek memoria galtzea edo kaltetutako gailua berrabiatzea eragin lezake, zerbitzuaren ukapen egoera sortuz (DoS). Ahultasun hau gertatzen da IKEv2 pakete batzuen prozesamendu oker batengatik. Erasotzaile batek ahultasun hori balia lezake IKEv2 pakete bat bidaliz kaltetutako gailu batera, prozesatuak izan daitezen. Eraso arrakastatsu bat izanez gero, kaltetutako gailuak memoria iraunkorki kontsumi dezan eragin liteke eta batzuetan berrabiatzeak gertatzea, eta horren ondorioz zerbitzuaren ukapen egoera sor liteke (DoS). Larritasun kritikoko ahultasun horretarako CVE-2018-0158 identifikatzailea erabili da.
- Eragiketen murrizketa okerra bufferraren memoriaren mugen barnean: Cisco IOS, Cisco IOS XE eta Cisco IOS XR softwarearen LLDP azpisistemak duen bufferraren gainezkatzearen ahultasun bat baliatuz, autentifikaziorik gabeko alboko erasotzaile batek zerbitzuaren ukapen egoera eragin lezake (DoS) edo altxatutako pribilegioekin kode arbitrarioa exekutatu. Larritasun kritikoko ahultasun horretarako CVE-2018-0167 identifikatzailea erabili da.
- Kanpoko iturrietatik datozen katea erako (string) parametroen erabilera okerra: Cisco IOS Software eta Cisco IOS XR Softwarearen LLDP azpisistemaren barnean kateak erabiltzeko moduak duen ahultasun bat baliatuz, alboko sare batera konektatutako erasotzaile batek, autentifikatuta egon behar izan gabe, Zerbitzuaren Ukapena eragin lezake edo altxatutako pribilegioekin kode arbitrarioa exekutatu. Larritasun altuko ahultasun horretarako CVE-2018-0175 identifikatzailea erabili da.
- Memoriaren bufferraren mugetan eragiketen murrizketa ezegokia: Cisco IOS Software eta Cisco IOS XR Softwarearen LLDP azpisistemak duen bufferraren gainezkatze erako ahultasun bat baliatuz, alboko sare batera konektatutako erasotzaile batek, autentifikatuta egon behar izan gabe, Zerbitzuaren Ukapena eragin lezake edo altxatutako pribilegioekin kode arbitrarioa exekutatu. Larritasun altuko ahultasun horretarako CVE-2018-0167 identifikatzailea erabili da.
- Ahultasuna akatsen erabilera eta kudeaketan (PK-ERRORS): Akatsak kudeatzeko moduan ahultasun bat dago BFD (Bidirectional Forwarding Detectio) protokoloaren goiburu bat osagabe dagoenean BFD pakete horren barnean. Urruneko erasotzaile batek, autentifikazioaren beharrik gabe, bereziki gaizki sortutako BFDF paketeak bidal litzake kaltetutako Switchean zehar, Zerbitzuaren Ukapena eraginez sistemaren nahitaezko berrabiatze batengatik. Larritasun altuko ahultasun horretarako CVE-2018-0155 identifikatzailea erabili da.

- Eragiketen murrizketa okerra bufferraren memoriaren mugen barnean: Cisco IOS eta Cisco IOS XEren zerbitzuaren kalitatearen azpisistemak (QoS) duen ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek zerbitzuaren ukapena (DoS) eragin lezake edo kode arbitrarioa exekutatu pribilegio gorenekin. Ahultasuna gertatzen da modu okerrean egiaztatzen direlako kaltetutako gailuaren 18999/udp atakara zuzenduta dauden paketeetako hainbat balio. Erasotzaile batek ahultasun hori balia lezake pakete gaiztoak bidaltzeko eta horiek prozesatzean bufferraren gainezkatze egoera gerta liteke. Ahultasun hau arrakastaz baliatuz gero, erasotzaileak kaltetutako gailuan kode arbitrarioa exekuta lezake pribilegio gorenekin. Era berean, erasotzaileak ahultasun hori balia lezake gailuak 'reload' eragiketa bat egin dezan. Ondorioz, epe baterako zerbitzuaren ukapen egoera sortuko litzateke, gailua berrabiatzen den bitartean. Larritasun kritikoko ahultasun horretarako CVE-2018-0151 identifikatzailea erabili da.

Ohartarazpen honetan azaldutako ahultasunetarako ondoko identifikatzaileak erreserbatu dira:

Rockwell Automation Stratix Industrial Managed Ethernet Switch: CVE-2018-0171, CVE-2018-0156, CVE-2018-0155, CVE-2018-0174, CVE-2018-0173, CVE-2018-0167, CVE-2018-0175

Rockwell Automation Stratix and ArmorStratix Switches: CVE-2018-0171, CVE-2018-0156, CVE-2018-0174, CVE-2018-0172, CVE-2018-0173, CVE-2018-0158, CVE-2018-0167, CVE-2018-0175

Rockwell Automation Stratix Services Router: CVE-2018-0158, CVE-2018-0151, CVE-2018-0167, CVE-2018-0175

**Etiketak:** Eguneraketa, Cisco, Sistema Eragilea, Ahultasuna

---

# Ahultasuna Siemensen iOS SIMATIC WinCC OA Operator Aplikazioan

**Argitaratze-data:** 2018/04/18

**Garrantzia:** Ertaina

**Kaltetutako baliabideak:**

- Siemensen SIMATIC WinCC OA Operator iOS App, bertsio guztiak.

**Azalpena:**

IOActive-ko Alexander Bolshev eta Emberdiko Ivan Yushkevich ikertzaileak Siemensekin batera koordinatu dira, ahultasun hori kudeatzeko. iOS SIMATIC WinCC OA Operator sistemarako aplikazioak ahultasun bat dauka eta gailu mugikorrerako sarbide fisikoa duen erasotzaile batek zifratu gabeko datuak irakur litzake, aplikazioaren direktorioaren barruan.

**Konponbidea:**

Siemensek honako konponbideak eta arintze espezifikoak identifikatu ditu, bezeroek arriskua murrizteko aplikatu ditzaketenak:

- Saio bakoitzaren hasieran eta ostean pasahitza gordetzeko aukera ematen duen botoia desaktibatu.
- SIMATIC WinCC OA sistemaren segurtasun-gidan jarraitu, SIMATIC WinCC OA sistemaren eremuan segurtasuna mantentzeko. Gida hau honako loturan deskargatu daiteke:

https://portal.etm.at/index.php?option=com_phocadownload&view=category&id=52:security&Itemid=81

**Xehetasuna:**

- Datu sentikorrak erakustea: Siemensen iOS SIMATIC WinCC OA Operator sistemarako aplikazioak ez dauka babes nahikorik aplikazioaren datu sentikor batzuk babesteko (zerbitzarira sartu ahal izateko datuak, esaterako). Gailu mugikorrerako sarbide fisikoa duen erasotzaile batek ahultasun hori baliatu dezake datu sentikorrak lortzeko, aplikazioaren direktorioaren barruan zifratuta ez daudenak. Ahultasun horretarako CVE-2018-4847 identifikatzailea erreserbatu da.

**Etiketak:** iOS, Mugikorrak, Siemens, Ahultasuna

---

# Buffer espazioak gainezka egin du ABBren CM600 eta SAB600 gailuetan

**Argitaratze-data:** 2018/04/19

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- SAB600 3.5
- SAB600 3.5.1
- PCM600 2.4
- PCM600 2.4.0.1
- PCM600 2.4.0.2
- PCM600 2.4.1
- PCM600 2.4.1.1
- PCM600 2.4.1.2
- PCM600 2.4.1.3

**Azalpena:**

Kaspersky Labs-eko Vladimir Dashchenkok bufferrak gainezka egitea eta antzeko ahultasun batzuk identifikatu ditu, ABBren CM600 eta SAB600 gailuei eragiten dietenak. Egiaztatu gabeko urrutiko erasotzaile batek sistema ustekabean ixtea eragin dezake edo kode arbitrarioa erabili.

**Konponbidea:**

ABB taldeak jakinarazi du ahultasunak produktu-bertsio hauek erabiliz konpontzen direla:

- PCM600 2.5 o ostekoa
- SAB600 4.0 o ostekoa

**Xehetasuna:**

Kaltetutako produktuetan gehitutako Sentinel HASP exekuzio-eremuak hainbat ahultasun ditu, hala nola bufferrak gainezka egitea, eta heap zein stack delakoei eragiten diete.  Erasotzaile bat ahultasunaz baliatu daiteke fitxategi gaizto bat Gemalto ACC (Admin Control Center) eremuan kargatzeko, bufferra gainezka eginaraziz. Gainezka egite horien ondorioz, urrutiko erasotzaileek kode arbitrarioa erabil dezakete edo urrutiko prozesua gelditu, zerbitzua ukatuz. Ahultasun horietarako CVE-2017-11498, CVE-2017-11497, CVE-2017-11496 identifikatzaileak erreserbatu dira.

**Etiketak:** Eguneratzea, Ahultasuna

---

# Schneider Electric erakundearen produktuen ahultasunak

**Argitaratze-data:** 2018/04/24

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- EVlink karga-estazioko webgunearen interfazea, v3.2.0-12_v1 bertsioaren aurreko guztiak.
- Wiser for KNX V2.1.0 eta aurrekoak.
- homeLYnk V2.0.1 eta aurrekoak.
- spaceLYnk V2.1.0 eta aurrekoak.

**Azalpena:**

Joakim B. Hellumek Schneider Electric etxeari eman dio tarteko larritasuna duen ahultasun baten berri. Pribilejioen eskalatze motakoa da eta horren ondorioz, erasotzaile batek administrazio baimenak lor litzake, urrutitik. Gainera, Jokin Guevara ikertzaile independenteak jakinarazi du larritasun handiko ahultasun bat dagoela, babestu gabeko FTP sarbide motakoa, Wiser for KNX gailuan (aurretik homeLYnk / spaceLYnk). Horren ondorioz, baimenik gabeko erasotzaile bat gailura sar liteke.

**Konponbidea:**

Schneider Electric etxeak partxe batzuk argitaratu ditu, azaldutako ahultasunak konpontzeko:

Pribilejioen eskalatzea:

https://www.schneider-electric.com/en/download/document/PHA6457000/

Babestu gabeko FTP sarbidea:

https://www.schneider-electric.com/en/download/document/FW2_1_1-HW_2_X_X-w4k/

**Xehetasuna:**

- EVlink karga estazioko cookie aldaketaren bidez, urrutiko erasotzaile batek administrari pribilejioak lor ditzake, urrutiko erasotzaileentzako egiaztatze zuzenik gabe. Ahultasun horretarako CVE-2018-7778 identifikatzailea erreserbatu da.
- FTP konfigurazio ahul edo babesik gabeko batek baimenik gabeko erasotzaile bati sarbidea ahalbidetu diezaioke. Ahultasun horretarako CVE-2018-7779 identifikatzailea erreserbatu da.

**Etiketak:** Eguneratzea, Nabigatzailea, Schneider Electric, Ahultasuna

---

# Hainbat ahultasun Advantech-en WebAccess HMI Designer sisteman

**Argitaratze-data:** 2018/04/24

**Garrantzia:** Ertaina

**Kaltetutako baliabideak:**

Advantech WebAccess HMI Designer

**Azalpena:**

Source Incite enpresako Steven Seeley ikertzaileak hainbat ahultasun atzeman ditu. Erasotzaile batek kodearen urrutiko exekuzioa burutu lezake kaltetutako produktuan.

**Konponbidea:**

Advantech etxeak ez du jakinarazi nola konpon daitezkeen atzemandako ahultasun horiek. Hala ere, deskubritu dituen ikertzaileak berak arintze estrategia bat gomendatu du: aplikazioaren interakzioa konfiantzazko fitxategietara mugatzea.

**Xehetasuna:**

- Kodearen urrutiko exekuzioa PM3 fitxategiak aztertzean edo PM2 artxiboa PM3 formatura bihurtzean. Urrutiko erasotzaile batek kode arbitrarioa exekutatu lezake, honakoren baten ondorioz:
  - Sarrera-datuak oker balioztatzea.
  - Erabiltzaileak emandako datuen luzera oker balioztatzea, luzera finkoko buffer batean kopiatu aurretik.
  - Objektu bat dagoen ez konprobatzea, horrengan eragiketak egin aurretik.

**Etiketak:** 0day, Ahultasuna

# Nonce berrerabiltzea BD Pyxis gailuetan

**Argitaratze-data:** 2018/04/25

**Garrantzia:** Ertaina

**Kaltetutako baliabideak:**

- BD Pyxis Anesthesia ES,
- BD Pyxis Anesthesia System 4000,
- BD Pyxis Anesthesia System 3500,
- BD Pyxis MedStation 4000 T2,
- BD Pyxis MedStation ES,
- BD Pyxis SupplyStation,
- BD Pyxis Supply Roller,
- BD Pyxis ParAssist System,
- BD Pyxis PARx,
- BD Pyxis CIISafe Workstation,
- BD Pyxis StockStation System, and
- BD Pyxis Parx handheld

**Azalpena:**

Mathy Vanhoef ikertzaileak (imec-DistriNet, KU Leuven) KRACK ahultasunak atzeman zituen eta BDk horien berri eman du. Erasotzaile batek trafiko datuak manipulatu litzake, komunikazio zifratuak partzialki agerraraziz edo trafiko injekzio bat eraginez.

**Konponbidea:**

BDk hirugarrenen partxeak ezarri ditu partxeen hedapenerako errutinaren bidez. Horrela, ahultasun hori konpontzen da ia gailu guztietan. Gailu batzuetarako BDrekin koordinatu beharra dago. BD bezeroekin jarri da harremanetan, partxeak programatu eta zabaltzeko. Gainera, zera gomendatzen du:

- Azken eguneratzeak Wifi sarbidea duten puntuetan instalatuta daudela ziurtatzea.
- Barruti fisikotik datozen erasoak prebenitzeko neurri fisiko egokiak aplikatzea.
- Datuen babes kopiak eta berreskuratze prozesuak badaudela egiaztatzea, hondamendiren bat gertatzekotan.

**Xehetasuna:**

Ahultasun bat dago WPA eta WPA2 protokoloan, industria osoan erabilia, KRACK (Key Reinstallation Attacks) deritzen berrinstalatze erasoek kaltetua.

Wi-Fi WPA eta WPA2 protokoloetan erabilitako lau urratsetan emandako establezimendu trafikoa manipulatu egin daiteke nonce delakoa berrerabiltzeko, gakoa berriro instalatuz. Horren ondorioz, erasotzaile bat seinalearen helmenaren barruan egon liteke, bitartekari erasoa egin eta tramak erreproduzitu, deszifratu edo faltsutu. Ahultasun honi honako identifikatzaileak esleitu zaizkio: CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087 y CVE-2017-13088.

**Etiketak:** Komunikazioak, Ahultasuna

# Vecna VGo Robot sistemetako ahultasunak

**Argitaratze-data:** 2018/04/25

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- VGo Robot, 3.0.3.52164 bertsioaren aurreko guztiak.

**Azalpena:**

Zingbox-eko Dan Regalado ikertzaileak hainbat ahultasun atzeman ditu, komando injekzio eta datuen transmisio motakoak, Vecnaren VGo Robot produktuei eragiten dietenak. Urrutiko erasotzaile batek sarean egindako firmware eguneratzeak bahitu litzake eta kodearen urrutiko exekuzioa burutu.

**Konponbidea:**

Vecnak gomendatutako eguneraketa bat argitaratu du, ahultasun horiek arintzeko. Eguneraketa prozesu hau gomendatzen du.

- VGo-k eguneratze automatikoak ditu aktibatuta, beraz, eguneratze guztiak automatikoki egiten dira, Interneterako sarbidea eskuragarri dagoenean. VGo itzalita edo erabiltzen ari bada, pantailan mezu bat agertuko da eta hurrengo erabileran eguneratu daitekeen galdetuko du.
- VGo unitate batek eguneratze automatikoak desaktibatuta baditu, eguneraketa ez da deskargatuko (hala ere, eguneratzeari buruzko abisu bat agertuko da VGo-ren pantailan). Vecnak gomendatzen du eguneraketa automatikoak aktibatuta edukitzeko.

**Xehetasuna:**

- Komandoen injekzioa: Ondoko sareetako erasotzaile batek komandoen injekzio bat burutu lezake. Ahultasun horretarako CVE-2018-8866 identifikatzailea erreserbatu da.
- Transmisioa: Erasotzaile batek firmware eguneraketak bahitu litzake ondoko sare batetik. Ahultasun horretarako CVE-2018-8860 identifikatzailea erreserbatu da.

**Etiketak:** Eguneratzea, Ahultasuna

# Bufferrak gainezka egitea Intel etxearen 2G-ko modemean

**Argitaratze-data:** 2018/04/25

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- Intel XMM71xx
- Intel XMM72xx
- Intel XMM73xx
- Intel XMM74xx
- Sofia 3G
- Sofia 3G-R
- Sofia 3G-R W

**Azalpena:**

Comsecuris enpresako Ralph Phillip Weinmann eta Nico Golde doktoreek bufferraren gainezkatze motako ahultasun horren berri eman diote Intel enpresari. Horrek, era berean, NCCIC zentroari jakinarazi dio. Urruneko erasotzaile batek ahultasun hori baliatu lezake kaltetutako gailuan urrunetik kodea exekutatzeko.

**Konponbidea:**

Intelek firmware bertsio berri bat argitaratu du, kaltetutako gailuetan ahultasuna zuzentzeko. Kaltetutako gailuak dituzten erabiltzaileek beren hornitzaileekin kontsultatu behar dute eguneraketa horren inguruan, ahalik eta arinen aplikatu ahal izateko.

**Xehetasuna:**

Urrutiko erasotzaile batek ETWS (Earthquake and Tsunami Warning System) prozesatze-moduluan dagoen bufferraren gainezkatze motako ahultasun hori baliatu lezake, ondoko sare baten bidez kode arbitrarioa erabiltzeko. Ahultasun horretarako CVE-2018-3624 identifikatzailea erreserbatu da.

**Etiketak:** Komunikazioak, Microsoft, Ahultasuna

---

# Schneider Electric erakundearen Pelco Sarix Pro kameren ahultasunak

**Argitaratze-data:** 2018/04/26

**Garrantzia:** Alta

**Kaltetutako baliabideak:**

- Firmwarea duen Pelco Sarix Pro sistemaren azken belaunaldia, 3.29.69aren aurreko bertsioa.

**Azalpena:**

Gulf Business Machines-eko Giri Veeraraghavan Veda ikertzaileak eta Weapon x taldeak Schneider Electric erakundeari jakinarazi diote mota honetako hiru ahultasun larri daudela: Bufferrak gainezka egitea, pribilegioetan eskalatzea eta informazioaren dibulgazioa. Pelco Sarix Pro kamerei eragiten diete. Egiaztatutako erasotzaile batek erabiltzaileen pasahitzak lor litzake, zerbitzua ukatu edo bufferrari gainezka eginarazi.

**Konponbidea:**

Schneider Electric erakundeak firmwarearen 3.29.69 bertsioa argitaratu du, ahultasun horiek konpontzeko. Deskarga egiteko:

https://www.pelco.com/search#keyword/v3.29.69/tab/documents

**Xehetasuna:**

Atzemandako ahultasunak honakoak dira:

- Bufferrak gainezka egitea: Bufferrak gainezka egin du cgi delakoaren ?set? programan. Ahultasun horretarako CVE-2018-7780 identifikatzailea erreserbatu da.
- Pasahitzak dibulgatzea eta pribilegioen eskalatzea: Egiaztatutako erasotzaile batek bereziki manipulatutako eskaerak bidal ditzake eta pasahitzak ikusi, pribilegioen eskalatzea ekarriz: Ahultasun horretarako CVE-2018-7781 identifikatzailea erreserbatu da.
- Pasahitzen dibulgazioa: Egiaztatutako erasotzaile batek pasahitzak ikus litzake. Ahultasun horretarako CVE-2018-7782 identifikatzailea erreserbatu da.

**Etiketak:** Eguneratzea, Schneider Electric, Ahultasuna

---

# Bufferrak gainezka egitea Delta Electronics erakundearen PMSoft delakoan

**Argitaratze-data:** 2018/04/27

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- PMSoft v 2.10 eta aurrekoak

**Azalpena:**

Ghirmay Desta ikertzaileak, Trend Microren Zero Day Initiative ekimenarekin lanean, bufferraren gainezkatze batzuen inguruan ohartarazi du, Delta Electronics erakundearen PMSoft sistemari eragiten diotenak. Erasotzaile batek ahultasun horiek baliatu litzake kode arbitrarioa erabiltzeko edo sistemari huts eginarazteko.

**Konponbidea:**

Delta Electronics erakundeak kaltetutako erabiltzaileei gomendatu die PMSoft v2.1 bertsiora eguneratzeko. 2018ko martxoaren 22tik dago eskuragarri. Deskarga lotura honen bidez egin daiteke:

www.deltaww.com/Products/PluginWebUserControl/downloadCenterCounter.aspx?DID=2092&DocPath=1&hl=en-US

**Xehetasuna:**

Aplikazioak bufferak gainezko egitearen estiloko hainbat ahultasun ditu. Esaterako, .ppm fitxategi batek bufferrak (PMSoften definitutakoa) irakur dezakeena baino balio luzeago bat sar dezake. Horren ondorioz, bufferra gainidazten da eta kode arbitrarioa exekutatu daiteke edo aplikazioari huts eginarazi. Ahultasun horretarako CVE-2018-8839 identifikatzailea erreserbatu da.

**Etiketak:** Eguneratzea, Ahultasuna

---

# Bufferrak gainezka egitea WECON Technology Co erakundearen LeviStudio HMI Editor eta PI Studio HMI Project Programmer sistemetan

**Argitaratze-data:** 2018/04/27

**Garrantzia:** Ertaina

**Kaltetutako baliabideak:**

- WECON LeviStudioU 1.10 bertsioa, WECON LeviStudioU 1.8.29 eta aurreko bertsioen osagaia.
- PI Studio HMI Project Programmer Build: 2017ko azaroaren 11koa eta aurrekoak.

**Azalpena:**

RVRTko Sergey Zelenyuk eta Leahy Center of Digital Investigation at Champlain Collegeko Michael DePlante ikertzaileek, Trend Microko Zero Day Initiative ekimenarekin batera, bufferraren gainezkatze bat atzeman dute. WECON Technology Co erakundearen LeviStudio HMI Editor eta PI Studio HMI Project Programmer sistemei eragiten die. Horren ondorioz, kodearen urrutiko exekuzioa burutu daiteke.

**Konponbidea:**

WECONek gomendatu du eskuragarri dagoen azken bertsioa deskargatzeko. Deskarga lotura honetan aurki daiteke:

http://wecon-disk.oss-ap-southeast-1.aliyuncs.com/LeviStudioU20180420 TEST.exe

**Xehetasuna:**

- Pilan oinarritutako buffer gainezkatzea: Bereziki manipulatutako fitxategi batek pila gainidaztea ekar dezake, aplikazio horien bidez zabaltzean, kodearen urrutiko exekuzioa gertatuta. Ahultasun horretarako CVE-2018-7527 identifikatzailea erreserbatu da.

**Etiketak:** Eguneratzea, Ahultasuna