
# 2018ko Abuztuaren Bulletina

## Ohartarazpenak - Kontrol Industrialeko Sistemak

---

## Pasahitzen hash ahula Davolink-en DVW-3200Nen

**Argitalpen data:** 2018/08/01

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- DVW-3200N, 1.00.06 bertsioaren aurreko guztiak

**Azalpena:**

NewSky Securityko Ankit Anubhavek pasahitzen hashen biltegiratze moduko ahultasun bat aurkitu du, ahalegin konputazional askirik gabe egindakoak. Urruneko erasotzaile batek gailuko pasahitzak eskura litzake.

**Konponbidea:**

Davolinkek ahultasun hau konpontzen duen firmwarearen bertsio berri bat argitaratu du. Hemen eskura daiteke: http://www.davolink.co.kr/sys/bbs/board.php?bo_table=0403&wr_id=50.

**Xehetasuna:**

Kaltetutako gailuek pasahitzen hash ahulak sortzen dituzte, erraz hautsi daitezkeenak, eta horrela erasotzaile batek gailuko pasahitzak eskura litzake. Ahultasun horretarako CVE-2018-10618 identifikatzailea erreserbatu da.

**Etiketak:** Ahultasuna

---

## Hainbat ahultasun AVEVA produktuetan

**Argitalpen data:** 2018/08/01

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- Wonderware License Server, v4.0.13100 bertsioa eta lehenagokoak (Flexara Imgrd erabiltzen du, 11.13.1.1 eta lehenagoko bertsioak). Soilik Counted Licenses ezaugarria 'ArchestrAServer.lic'-ekin duten erabiltzaileak daude kaltetuta.
- InTouch Access Anywhere 2017 Update 2 eta lehenagokoak. jQueryren bertsio ahulak 3.0.0 baino lehenagokoak dira.

**Azalpena:**

Googlen Security Team-ek eta ikertzaile anonimo batek hainbat ahultasun identifikatu dituzte AVEVA produktuetan. Sarbide datuen neutralizazio ezegokiaren erakoak eta memoriaren bufferraren mugetan murrizketa ezegokiaren erakoak dira. Erasotzaile batek informazio sentikorra eskura lezake, Javascript eta HTML kodea exekutatu edo urruneko kodea ere administratzaile pribilegioekin.

**Konponbidea:**

AVEVAk kaltetutako erabiltzaileei gomendatzen die 'InTouch Access Anywhere 2017 Update 2b' eta 'Hotfix Wonderware License Server VU-485744' partxeak edo ondorenekoak instalatzea, kaltetutako produktuaren arabera. **Xehetasuna:**

- Memoriaren bufferraren mugetan murrizketa ezegokia. Imgrd-n bufferraren gainezkatzea eta Flexera FlexNet Publisher-en Vendor Daemon baliatuz urruneko erasotzaile batek kode arbitrarioa exekuta lezake manipulatutako pakete baten bidez, eta horrela urrunetik kodea exekuta liteke administratzaile pribilegioekin. Ahultasun horretarako CVE-2015-8277 identifikatzailea erabili da.
- Web orria sortzean sarrera datuen neutralizazio desegokia (cross-site scripting): jQuery liburutegiak cross-site scripting (XSS) erasoak jasotzeko arriskua du domeinu gurutzatuko Ajax eskaera bat dataType aukera gabe egiten denean, eta horrek testu/javascript erako erantzunak exekutatzea eragiten du. Ahultasun horretarako CVE-2015-9251 identifikatzailea erabili da.

**Etiketak:** Eguneraketa, Ahultasuna

# Informazioaren zabalkundea Johnson Controls-en Metasys eta BCPro-n

**Argitalpen data:** 2018/08/01

**Garrantzia:** Ertaina

**Kaltetutako baliabideak:**

- Metasys System, 8.0 bertsioa eta lehenagokoak
- BCPro (BCM), 3.0.2 bertsioaren aurreko guztiak

**Azalpena:**

Zingbox-eko Dan Regalado ikertzaileak informazioaren zabalkunde erako ahultasun bat identifikatu du, Johnson Controls-en produktuei eragiten diena. Erasotzaile batek informazio teknikoa eskura lezake.

**Konponbidea:**

Metasys-en ahultasuna v8.1 bertsioan zuzendu zen, baina hala ere, produktuaren azken bertsiora, 9.0ra, eguneratu beharra dago. Ahultasuna konpontzeko BCPro Workstationeko erabiltzaileek v3.0 bertsiora eguneratu beharra dute eta BACnet Router eta Gatewaykoek 3.0.2 bertsiora.

**Xehetasuna:**

Ahultasun hau HTTPn oinarritzen diren zerbitzariarekiko komunikazioen akatsen kudeaketa desegokiaren ondorioa da, eta horrek eragin lezake erasotzaile batek informazio teknikoa eskuratu ahal izatea. Ahultasun horretarako CVE-2018-10624 identifikatzailea erabili da.

**Etiketak:** Komunikazioak, Ahultasuna

# Hainbat ahultasun Delta Electronics-en CNCSoft eta ScreenEditor-en

**Argitalpen data:** 2018/08/08

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- CNCSoft, 1.00.83 bertsioa eta lehenagokoak
- ScreenEditor, 1.00.54 bertsioa

**Azalpena:**

Mat Powell-ek, Trend Microko Zero Day Initiativerekin lankidetzan ahultasun hauen berri eman dio NCCIC/ICS-CERTi. Horiek arrakastaz baliatuz erasotzaile batek urrunetik kodea exekuta lezake administratzaile pribilegioekin.

**Konponbidea:**

Delta Electronicsek CNCSoften azken bertsiora eguneratzea gomendatzen du, v1.01.09, eta aplikazioaren interakzioa konfiantzako fitxategietara murriztea.

**Xehetasuna:**

- Pilan oinarritutako bufferraren gainezkatzearen hainbat ahultasunek softwareak huts egitea eragiten dute. Proiektuko fitxategietako datuak pilara kopiatu baino lehen erabiltzailearen sarbidea ez egiaztatzeagatik gertatzen da hori. Ahultasun horretarako CVE-2018-10636 identifikatzailea erabili da.
- Mugez kanpoko irakurketa erako bi ahultasunek ustekabeko itxiera eragiten dute. Proiektuko fitxategiak prozesatzeko erabiltzailearen sarbidea ez egiaztatzeagatik gertatzen da hori. Ahultasun horretarako CVE-2018-10598 identifikatzailea erabili da.

**Etiketak:** Ahultasuna

# Hainbat ahultasun Medtronic produktuetan

**Argitalpen data:** 2018/08/08

**Garrantzia:** Ertaina

**Kaltetutako baliabideak:**

- MMT - 508 MiniMed insulin pump
- MMT - 522 / MMT - 722 Paradigm REAL-TIME
- MMT - 523 / MMT - 723 Paradigm Revel
- MMT - 523K / MMT - 723K Paradigm Revel
- MMT - 551 / MMT - 751 MiniMed 530G
- 24950 MyCareLink Monitor, bertsio guztiak.
- 24952 MyCareLink Monitor, bertsio guztiak.

**Azalpena:**

Whitescope LLCko Billy Riosek, Jesse Youngek eta Jonathan Buttsek ahultasun hauen berri eman diote NCCIC/ICS-CERTi. Horiek baliatuz

urruneko erasotzaile batek atzemandako hari gabeko komunikazioak berrinjekta litzake eta paziente bati intsulina (bolus) ematea eragin lezake. Bestalde, erasotzaile batek MyCareLink gailuetara sarbide fisikoa lortuko balu, produktu bakoitzaren kredentzialak eskuratzeko gai izango litzateke. Ondoren, ahultasun hori balia liteke Medtronic CareLinken sarera datu okerrak kargatzeko.

**Konponbidea:**

- MMT gailuei eragiten dieten ahultasunei dagokienez, Medtronicek ez du horientzako eguneraketarik garatuko, erabiltzaile batek inoiz ez badu urruneko kontrolik programatu edo erabili ez baitu erasorik jasateko arriskurik. Gainera, erabiltzaileak urruneko aukera desaktibatzen badu edo bere intsulina bonban 'easy bolus' aukera desaktibatzen badu, erasorik jasateko arriskurik ez luke.
- MyCareLink Monitor gailuei eragiten dieten ahultasunei dagokienez, Medtronicek zerbitzariaren eguneraketak egin ditu ohar honetan egiaztapen askiez modura identifikatutako ahultasunari aurre egiteko. Gainera, zerbitzariaren aldean arintze osagarriak ezartzen ari da datuen integritatea eta egiazkotasuna hobetzeko. Bestalde, Medtronicek erabiltzaileei aholkatzen die babes neurri osagarriak hartzea, ahultasun hauek baliatzeko arriskua murriztearren. Zehazki, erabiltzaileek honakoa egin behar lukete:
  - Etxeko monitorearen kontrol fisiko egokia izatea.
  - Soilik osasun arretako hornitzailearen edo Medtroniceko ordezkari baten aldetik zuzenean eskuratutako etxeko monitoreak erabiltzea, sistemaren integritatea bermatzearren.
- Azkenik, Medtronicek argitaratutako informazio gehiago ondoko loturan aurki daiteke: https://www.medtronic.com/security

**Xehetasuna:**

- MNT modeloetan bonbaren eta hari gabeko osagarrien arteko komunikazioak testu gardenaren bidez transmititzen dira. Gaitasun nahikoa lukeen erasotzaile batek transmisio horiek atzeman litzake eta informazio sentikorra atera, esate baterako gailuaren serie zenbakiak. Ahultasun horretarako CVE-2018-10634 identifikatzailea erabili da.
- Goian identifikatutako MMT gailuak urruneko kontrolagailu batekin parekatzen direnean eta 'easy bonus' eta 'remote bolus' aukerak aktibatuta dituztenean (ez baitira aukera lehenetsiak), atzemate-errepikatze erako eraso bat jasateko arriskua dute. Erasotzaile batek urruneko kontrolagailuaren eta bonbaren arteko hari gabeko komunikazioak atzeman litzake eta horiek errepikatu, intsulina bolo bat bana dadin eragiteko. Ahultasun horretarako CVE-2018-12781 identifikatzailea erabili da.
- Kaltetutako MyCareLink produktuen eguneraketen zerbitzuak ez du aski egiaztatzen kargatutako datuen benetakotasuna. Monitorearen produktukako kredentzialak eta gailu kardiako ezargarriaren informazioa eskuratuko lituzkeen erasotzaile batek datu ez baliagarriak karga litzake Medtronic CareLinken sarean. Ahultasun horretarako CVE-2018-10626 identifikatzailea erabili da.
- Kaltetutako MyCareLink Monitor produktuek produktu bakoitzean erabiltzen dituzten kredentzialak formatu eskuragarri batean gordetzen dituzte. Erasotzaile batek kredentzial horiek erabil litzake sarean autentifikatzeko eta datu lokalak enkriptatzeko geldirik daudenean. Ahultasun horretarako CVE-2018-10622 identifikatzailea erabili da.

**Etiketak:** Ahultasuna

---

# Hainbat ahultasun Siemensen produktuetan

**Argitalpen data:** 2018/08/08

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- Automation License Manager 5, 5.3.4.4 bertsioa baino lehenagoko guztiak.
- Automation License Manager 6, 6.0.1 bertsioa baino lehenagoko guztiak (CVE-2018-11455 ahultasunak soilik kaltetua).
- SIMATIC STEP 7 (TIA Portal) eta WinCC (TIA Portal) V10, V11, V12, bertsio guztiak.
- SIMATIC STEP 7 (TIA Portal) eta WinCC (TIA Portal) V13, bertsio guztiak.
- SIMATIC STEP 7 (TIA Portal) eta WinCC (TIA Portal) V14, V14 SP1 Update 6 bertsioa baino lehenagoko guztiak.
- SIMATIC STEP 7 (TIA Portal) eta WinCC (TIA Portal) V15, V15 Update 2 bertsioa baino lehenagoko guztiak.
- MindConnect IoT2040, V03.01 bertsioa baino lehenagoko guztiak.
- MindConnect Nano (IPC227D), V03.01 bertsioa baino lehenagoko guztiak.
- SIMATIC ET 200SP Open Controller CPU 1515SP PC (OC1), V2.1 bertsioa baino lehenagoko guztiak.
- SIMATIC HMI WinCC Flexible, bertsio guztiak.
- SIMATIC IPC DiagBase, bertsio guztiak.
- SIMATIC IPC DiagMonitor, bertsio guztiak.
- SIMATIC S7-1200, bertsio guztiak.
- SIMATIC S7-1500, V2.5.2 bertsioa baino lehenagoko guztiak.
- SIMATIC S7-1500 Software Controller, bertsio guztiak.
- SIMATIC WinCC OA V3.14, bertsio guztiak.
- SIMATIC WinCC OA V3.15, bertsio guztiak.
- SIMATIC WinCC OA V3.16, bertsio guztiak.
- SINUMERIK Integrate Access MyMachine service engineer client, Sinumerik Integrate Product suitearen zati modura, V4.1.7 bertsioa eta lehenagokoak kaltetuta.
- SINUMERIK Integrate Operate Client, Sinumerik Integrate Product suitearen zati modura, 2.0.11/3.0.11 bertsioak eta horiek baino lehenagoko guztiak.

**Azalpena:**

Kaspersky Lab-eko Vladimir Dashchenko eta Nozomi Networkseko Younes Dragoni ikertzaileek, ICS-CERTeko lantaldeak eta Siemensek hainbat ahultasunen aurkikuntzan eta kudeaketan parte hartu dute. Era honetakoak dira: direktorio jauzia, baimenen kudeaketa desegokia, bereziki diseinatutako paketeen bidalketa eta OpenSSLrekin zerikusia duten arazoak. OpenSSLrekin zerikusia duen ahultasuna baliatuz urruneko erasotzaile batek kanal 'seguru' batean OpenSSLrekin eskualdatutako informazioa lor lezake, konfidentzialtasuna arriskuan jarriz. Bestalde, gainerako bi ahultasunak baliatuz, kaltetutako gailuetan erasotzaile batek urrunetik kodea exekuta lezake edo direktorioen egitura aldatu.

**Konponbidea:**

Ahultasunak arintzen dituen softwarearen bertsio berria eskuragarri dago ondoko produktuen kasuan:

- Automation License Manager 5, V5.3.4.4 bertsiora eguneratu.
- Automation License Manager 6, V6.0.1 bertsiora eguneratu.

Kaltetutako produktua ezin bada eguneratu, fabrikatzaileak gomendatzen du software hau daukan sistemara sartzeko erabiltzen den sarerako sarbidea murriztea.

- SIMATIC STEP 7 (TIA Portal) eta WinCC (TIA Portal) V14, V14 SP1 Update 6 bertsiora eguneratu.
- SIMATIC STEP 7 (TIA Portal) eta WinCC (TIA Portal) V15, V15 Update 2 bertsiora edo ondorenekoetara eguneratu.
- Kaltetuta dauden SIMATIC STEP 7 (TIA Portal) eta WinCCren (TIA Portal) 10, 11, 12 eta 13. bertsioen kasuan, fabrikatzaileak ondoko arintzeak ezartzea gomendatzen du:
  - Sistema eragilerako sarbidea soilik baimendutako pertsonek izatea.
  - GSD fitxategiak balioztatzea beren zilegitasuna egiaztatzeko eta soilik iturri fidagarrietako GSD fitxategiak prozesatzea.

- MindConnect IoT2040, V03.01 bertsiora edo berriagoetara eguneratzea Mindsphere web frontend-ekin.
- MindConnect Nano (IPC227D), V03.01 bertsiora edo berriagoetara eguneratzea Mindsphere web frontend-ekin.
- SIMATIC S7-1500, V2.5.2 bertsiora eguneratzea.
- SINUMERIK Integrate Access MyMachine service engineer client, V4.1.8 bertsiora eguneratzea, Sinumerik Integrate Product suitearen azken bertsioa eguneratuz.
- SINUMERIK Integrate Operate Client, V2.0.12/3.0.12 bertsiora eguneratzea, Sinumerik Integrate Product suitearen azken bertsioa eguneratuz.
- S7-1200. Fabrikatzaileak gomendatzen du web zerbitzaria desgaitzea ez bada erabiltzen ari, edo zerbitzarirako sarbidea murriztea Ethernet/PROFINET ataka/interfazearen bidez posible bada. Konfigurazioak 'General/Web server access'-en egin daitezke.
- Arintzeetan oraindik aipatu ez diren gainerako produktuetarako, fabrikatzaileak gomendatzen du kaltetutako gailuetarako sarbidea murriztea baliabide egokiak erabiliz, adibidez suebaki baten konfigurazioa.

**Xehetasuna:**

- **Direktorio jauzia** (Automation License Manager). Ahultasun hau arrakastaz baliatuz gero, erasotzaile batek fitxategiak modu arbitrarioan mugi litzake eta urrunetik kodea ere exekuta lezake agian, sistemaren konfidentzialtasuna, integritatea eta eskuragarritasuna arriskuan jarriz. Ahultasun hau baliatu ahal izateko beharrezkoa da erasotzailea kaltetutako produktuaren sare berean egotea, pribilegiorik edo sistemaren baldintza berezirik behar izan gabe, baina beharrezkoa izanik erabiltzaile biktima baten interakzioa. Ahultasun horretarako CVE-2018-11455 identifikatzailea erabili da.
- **Bereziki diseinatutako paketeen bidalketa** (Automation License Manager). Kaltetutako produktua dagoen sarera sarbidea lukeen erasotzaile batek bereziki diseinatutako paketeak bidal litzake jakiteko ea posible den urruneko beste sistema bateko sare ataka batera sartzea. Horren bitartez erasotzaileak sarearen eskaneatze oinarrizko bat egin dezake makina biktima bat erabiliz informazioa eskuratzeko. Ahultasun hau baliatzeko erasotzaileak kaltetutako produktua dagoen sare berera konektatuta egon behar du, ez du pribilegiorik behar, eta ez da beharrezkoa erabiltzaileekin interaktuatzea. Ahultasun horretarako CVE-2018-11456 identifikatzailea erabili da.
- **Baimenen kudeaketa desegokia.** TIA Portal-en lehenetsitako instalazioan fitxategi batzuek dauzkaten baimenek sistemara sarbide lokala duen erasotzaile bati ahalbidetuko liokete bereziki diseinatutako fitxategiak sartzea. Horrela TIA Portal abiatzea eragotz daiteke eta ondorioz zerbitzuaren ukapena eragin edo kode gaiztoa lokalki exekutatu. Ahultasun hau arrakastaz baliatzeko ez da behar baimen berezirik, baina beharrezkoa da biktima saiatzea TIA Portal abiatzen fitxategien manipulazioa gertatu ondoren. Ahultasun horretarako CVE-2018-11453 identifikatzailea erabili da.
- **Baimenen kudeaketa desegokia.** TIA Portalen lehenetsitako instalazioan fitxategi batzuek dauzkaten baimenek erasotzaile bati ahalbidetuko liokete, sistemara sarbide lokala baldin badu, beste gailu batzuetara transferituak izan daitezkeen baliabideak manipulatzea, ondoren exekutatuak izateko. Ahultasun hau arrakastaz baliatzeko ez da baimen berezirik behar, baina beharrezkoa da manipulatutako fitxategiak biktimak transferitzea beste gailu batera (PG). Ahultasun horretarako CVE-2018-11454 identifikatzailea erabili da.
- **OpenSSL**. OpenSSL v1.0. 'error state'-erako mekanismo bat jarri zen. Mekanismo horrek ez du ondo funtzionatzen SSL_red() edo SSL_write() funtzioei dei egiten zaienean. Horren ondorioz gerta liteke SSL/TLS geruzan zifratu gabeko datuak bidaltzea. Ahultasun hori arrakastaz baliatu ahal izateko beharrezkoa da erasotzaile batek akats bat eragitea SSL/TLSren baitako konexioa ezartzen den bitartean (handshake) eta aplikazioak akatsa jaso ondoren egitea deiak SSL_read() edo SSL_write()-ri. Ahultasun hau baliatzeko ez da pribilegiorik edo erabiltzearen interakziorik behar. Ahultasun horretarako CVE-2017-3737 identifikatzailea erabili da.

**Etiketak:** Nabigatzailea, Pribatutasuna, Siemens, Ahultasuna

---

# Hainbat ahultasun Zipato-ren Zipabox-en

**Argitalpen data:** 2018/08/09

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- Zipato Zipabox (smart home controller)

**Azalpena:**

Kaspersky Lab ICS CERTen Critical Infrastructure Defense Teameko Andrey Muravitskyk hainbat ahultasunen berri eman dio Zipatori. Urruneko erasotzaile batek informazio sentikorra lor lezake eta horrekin erasoaren azalera zabaldu, ahultasun bat baliatu edo, autentifikatu gabe, testu gardeneko pasahitzak eskuratu. Are gehiago, kaltetutako gailuek kudeatzen duten etxe inteligente osoaren kontrola hartzera irits liteke.

**Konponbidea:**

Oraingoz ez dago inolako konponbiderik eskuragarri.

**Xehetasuna:**

- **Informazioa sentikorraren zabalkundea:** autentifikatu gabeko erasotzaile batek eskuragarri dauden Zipabox gailuei buruzko informazio sentikorra eta bere informazio teknikoa lor lezake. Ahultasun horretarako CVE-2018-15125 identifikatzailea erabili da.
- **Hash ahuleko algoritmoa:** autentifikaziorik gabeko erasotzaile batek ahultasun hau balia lezake testu gardeneko pasahitzak lortzeko. Ahultasun horretarako CVE-2018-15124 identifikatzailea erabili da.
- **Konfigurazioaren biltegiratze ez segurua:** autentifikaziorik gabeko erasotzaile batek ahultasun hau balia lezake etxe inteligente osoaren kontrola hartzeko. Ahultasun horretarako CVE-2018-15123 identifikatzailea erabili da.

**Etiketak:** Pribatutasuna, Ahultasuna

---

# Hainbat ahultasun NetComm Wireless-en 4G LTE Light Industrial M2M routerrean

**Argitalpen data:** 2018/08/10

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- 4G LTE Light Industrial M2M routerra (NWL-25), firmwarearen 2.0.29.11 bertsioa eta lehenagokoak.

**Azalpena:**

Aditya K. Sood ikertzaileak Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF) eta informazio sentikorraren agerpen erako hainbat ahultasunen berri eman dio ICS-CERTi, NetComm Wireless fabrikatzailearen 4G LTE Light Industrial M2M routerrari eragiten diotenak. Ahultasun horiek arrakastaz baliatuz gero, urruneko erasotzaile batek informazio sentikorra lor lezake kaltetutako gailutik.

**Konponbidea:**

NetComm Wirelessek firmware bertsio berri bat argitaratu du (NWL-25, 2.0.29.12_C firmware bertsioa) 4G LTE Light Industrial M2M routerrari eragiten dioten ahultasunak konpontzeko.

Deskargarako lotura: https://support.netcommwireless.com/product/nwl-25#Firmware

**Xehetasuna:**

- Gailuak konfigurazio fitxategi eta profiletara sartzen uzten du erabiltzailea erregistraturik egon behar izan gabe. Ahultasun horretarako CVE-2018-14782 identifikatzailea erabili da.
- Gailuak ez du segurtasun neurririk saioen tratamendurako. Hori baliatuz erasotzaile batek bereziki sortutako eskaera bat bidal lezake, kaltetutako produktuaren barnean erregistratuta dagoen biktima batek gailuaren pasahitza urrunetik alda dezan. Ahultasun horretarako CVE-2018-14783 identifikatzailea erabili da.
- Cross-site scripting-erako ahultasun bat baliatuz urruneko erasotzaile batek kode arbitrarioa exekuta lezake gailuan. Ahultasun horretarako CVE-2018-14784 identifikatzailea erabili da.
- Gailuak duen fitxategien direktorioa eskuragarri dago autentifikazioaren beharrik gabe. Erasotzaile batek ahultasun hori balia lezake kaltetutako gailuaren informazioa eskuratzeko eta eraso konplexuagoak prestatzeko. Ahultasun horretarako CVE-2018-14785 identifikatzailea erabili da.

**Etiketak:** Edukien kudeatzailea, Nabigatzailea, Pribatutasuna, Ahultasuna

---

# Hainbat ahultasun Crestron-en TSW-X60 eta MC3-n

**Argitalpen data:** 2018/08/10

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- TSW-X60, 2.001.0037.001 bertsioaren aurreko guztiak
- MC3, 1.502.0047.001 bertsioaren aurreko guztiak

**Azalpena:**

Jackson Thuraisamyk, Security Compassekin lankidetzan, ahultasun hauetako batzuen berri eman dio Crestroni. Bestalde, Ricky 'HeadlessZeke' Lawshae-k, Trend Microko Zero Day Initiativerekin lankidetzan, ahultasun gehiagoren berri eman dio NCCIC/ICS-CERTi. Ahultasun horiek arrakastaz baliatuz gero urrunetik kodea exekuta liteke sisteman pribilegioen eskalatzea lortuz.

**Konponbidea:**

Crestonek erabiltzaileei aholkatzen die beren gailuak firmwarearen azken bertsiora eguneratzea. Hemen dago eskuragarri:

- TSW-X60 (saio hasiera nahitaezkoa): https://www.crestron.com/en-US/Software-Firmware/Firmware/Touchpanels/TSW-560-TSW-760-TSW-1060/2-001-0040-01
- MC3 (saio hasiera nahitaezkoa): https://www.crestron.com/en-US/Software-Firmware/Firmware/Touchpanels/TSW-560-TSW-760-TSW-1060/2-001-0040-01

Azkenik, Crestonek erabiltzaileei onlineko laguntza kontsultatzea ere aholkatzen die, ahultasun honi eta beste batzuei buruzko informazioa eskuratzearren (#5471 artikulua). Gailuak gotortzeko informazioa #5571 artikuluan dago eskuragarri.

**Xehetasuna:**

- Sistema Eragilean komandoen injekzio erako ahultasun bat baliatuz, autentifikatu gabe kodea urrunetik exekuta liteke Crestron Toolbox Protocol-en (CTP) Bash Shell zerbitzu baten bidez. Ahultasun honek TSW-X60 gailuei soilik eragiten die. Ahultasun horretarako CVE-2018-11228 identifikatzailea erabili da.
- Sistema Eragilean komandoen injekzio erako ahultasun bat baliatuz, autentifikatu gabe kodea urrunetik exekuta liteke Crestron Toolbox Protocol-en (CTP) komandoak injektatuz. Ahultasun honek TSW-X60 gailuei soilik eragiten die. Ahultasun horretarako CVE-2018-11229 identifikatzailea erabili da.
- Fabrikatzaileak gailuak bidaltzen ditu autentifikazioa desgaiturik dutela, eta ez dago inolako ohartarazpenik erabiltzaileek segurtasun neurriak ezar ditzaten eta aukera hori gaitu dezaten. Eragindako gailua arriskuan dagoenean, CTP kontsolarako sarbidea irekita gelditzen da. Ahultasun horretarako CVE-2018-10630 identifikatzailea erabili da.
- Administrazio kontuen pasahitzak zein diren asma daiteke pribilegio normalak dituzten erabiltzaileek eskura dezaketen informazioa baliatuz. Erasotzaileek pasahitz horiek deszifra litzakete eta ondoren ezkutuko API deiak exekutatu, eta pribilegio altuekin CTP kontsolak duen sandboxetik ihes egingo lukete. Ahultasun horretarako CVE-2018-13341 identifikatzailea erabili da.

**Etiketak:** Ahultasuna

---

# Hainbat ahultasun Moxa produktuen Intel Management Engine-n

**Argitalpen data:** 2018/08/10

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- DA-820 Series, V1.10S03 baino lehenagoko bertsioak
- MC-7200-DC-CP Series, V1.20S01 baino lehenagoko bertsioak
- MC-7200-MP Series, V1.30S01 baino lehenagoko bertsioak
- EXPC-1519 Series, V1.20S02 baino lehenagoko bertsioak
- DA-720 Series, V1.30S00 baino lehenagoko bertsioak

**Azalpena:**

Moxak bere portfolioko produktuen artetik Intel Management Engineren ahultasunek (CVE-2017-5689, CVE-2017-5705, CVE-2017-5708, CVE-2017-5711, CVE-2017-5712) eragindakoak identifikatu ditu eta produktu bakoitzerako BIOSaren eguneraketa bat argitaratu du, ahultasun horiek konpontzen dituena.

**Konponbidea:**

Moxak bere produktuen artetik kaltetuta daudenak identifikatu ditu eta firmware eguneraketa argitaratu du. Zerrendan ez dauden produktuei ez diete eragiten dokumentu honetan aipatutako ahultasunek. Produktu kaltetuak erosi dituzten pertsonei Moxak aholkatzen die Moxaren Arreta zerbitzu orokorraren bidez laguntza jasotzeko eta BIOSaren azken bertsiora eguneratzeko:

- DA-820 Series, V1.10S03 baino lehenagoko bertsioak
- MC-7200-DC-CP Series, V1.20S01 baino lehenagoko bertsioak
- MC-7200-MP Series, V1.30S01 baino lehenagoko bertsioak
- EXPC-1519 Series, V1.20S02 baino lehenagoko bertsioak
- DA-720 Series, V1.30S00 baino lehenagoko bertsioak

**Xehetasuna:**

2017ko maiatzean hainbat ikertzailek ahultasun baten berri eman zuten. Horren arabera, sare batera sarbiderik izan behar ez lukeen erasotzaile batek sistemaren pribilegioak eskura litzake Intelen administrazio SKUak emateko eta erasotzaile lokal batek administrazio funtzioak eman litzake sare edo sistema lokalaren pribilegioak lortzeko Intelen administrazio SKUn. 2017ko bigarren seihilekoan ikertzaileek Intel Management Enginerekin zerikusia zuten hainbat ahultasun aurkitu zituzten (CVE-2017-5705, CVE-2017-5708, CVE-2017-5711, CVE-2017-5712).

**Etiketak:** Ahultasuna

---

# Autentifikazioari ihes egitea ABBren eSOMS-en

**Argitalpen data:** 2018/08/13

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- eSOMS, 6.0.2 bertsioa

**Azalpena:**

Ikertzaile anonimo batek autentifikazioari ihes egitearen erako ahultasun baten berri eman du, ABBren eSOMS produktuei eragiten diena. Aplikaziora sartzea ahalbidetu lezake erabiltzaile legitimo modura.

**Konponbidea:**

Ahultasun hau konponduko duen 6.0.3 partxea prestatzen ari da ABB. Egiaztapen bat gehituko dio eta horrek ez du utziko SOMSen autentifikatzen, LDAP zerbitzariaren konfiguraziotik independentea den pasahitzik gabe.

Bitartean bezeroei aholkatzen zaie 'Unauthenticated Authentication' aukera desgaituta dagoela ziurtatzea LDAP konfigurazioaren aukeretan. Ziurtatu beharra dago eSOMSen web.config fitxategian soilik ondoko balioak daudela konfiguratuta: ? 'LDAP_Path', 'LDAP_User_Search' eta 'LDAP_SSL_Enabled'.

**Xehetasuna:**

LDAP autentifikazio zerbitzariak konfiguratu daitezke autentifikazio anonimoa baimentzeko. eSOMSen LDAP autentifikazioa konfiguratzen denean, erabiltzaile batek pasahitzik gabe saioa has dezake ondorengo aukerak konfiguratuta badaude:

- LDAP zerbitzaria konfiguratuta dago 'Unauthenticated Authentication' baimentzeko
- web.config fitxategian balio giltzarri gehiago konfiguratzen direnean, honako hauez gain: 'LDAP_Path', 'LDAP_User_Search' eta 'LDAP_SSL_Enabled'.

**Etiketak:** Ahultasuna

---

# Zerbitzu ukapena Phoenix Contact-en ILC 1x1 ETH-n

**Argitalpen data:** 2018/08/14

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- Phoenix Contact ILC 131, 151, 171, 191 ETH, bere firmwarearen bertsio guztietan.

**Azalpena:**

Hochschule Augsburgeko Matthias Niedermaier eta Florian Fischer-ek eta Berlineko Freie Universitäteko Jan-Ole Malchow-ek zerbitzu ukapen erako ahultasun baten berri eman dute. Erasotzaile batek gailua dagoen sarea satura dezake, gailua bera abiatzea eragotziz.

**Konponbidea:**

Phoenix Contact ILC 1x1 erabiltzen duten bezeroei aholkatzen zaie gailuak sare itxietan erabiltzea edo suebaki egoki batez babesturik.

Sareko gailuak babesteko neurriei buruzko informazio xehea eskuratzeko, Phoenix Contactek ondoko lotura aztertzea gomendatzen du:

https://www.phoenixcontact.com/assets/downloads_ed/local_pc/web_dwl_technical_info/ah_en_industrial_security_107913_en_01.pdf

**Xehetasuna:**

IEC 61131 programaren prozesamendua oso geldoa izan daiteke eta gelditu ere egin daiteke sareak duen trafikoa oso handia bada.

Sareko kargaren prozesamenduak CPUren horrenbesterainoko potentzia behar duenez, gailuaren funtzio guztien operazioak moteldu egingo dira, 61131 programa barne. Horrek automatizazioaren egitekoari eragin diezaioke. Sarearen saturazioa deuseztatzen den unean ILC gailua bere egoera normalera itzultzen da.

**Etiketak:** Komunikazioak, Ahultasuna

---

# Hainbat ahultasun Philipsen IntelliSpace Cardiovascular-en

**Argitalpen data:** 2018/08/16

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- IntelliSpace Cardiovascular (ISCV), 3.1 eta lehenagoko bertsioak.
- Xcelera, 4.1 eta lehenagoko bertsioak.

**Azalpena:**

Philipsek hainbat ahultasunen berri eman du informazioaren kudeaketarako IntelliSpace Cardiovascular (ISCV) produktuetan. Sarbide lokala lukeen eta aplikazioan autentifikatuta legokeen erasotzaile batek ahultasun horiek balia litzake pribilegioak eskalatzeko ISCV/Xcelera zerbitzariaren barnean edo kode arbitrarioa exekutatzeko.

**Konponbidea:**

- ISCVren 2.X eta lehenagoko bertsioei eragiten dien argitaratutako ahultasunetako bat 3.1 bertsioan zuzendua izan da. Erabiltzaileak harremanetan jar daitezke Philipsen laguntza ekipoarekin bere eguneraketarako.
- 3.1 eta lehenagoko bertsioari buruzko ahultasunaren eta Xceleraren 4.1 eta lehenagoko bertsioen kasuan, 2018ko urrirako espero da hura konponduko duen eguneraketa bat.
- 3.2 bertsioa aplikagarria izan baino lehen eta arintze neurri modura, Philipsek ondokoa gomendatzen die erabiltzaileei:
  - Fitxategien gaineko sarbide eta baimen politikak berrikustea, ahal den heinean baimen horiek murriztuz.

**Xehetasuna:**

- Pribilegioen kudeaketa desegokia: ISCVren 2.X eta lehenagoko bertsioetan eta Xcelera-ren 4.X, 3X eta lehenagoko bertsioetan, erabiltzaile autentifikatu batek sarbidea izan dezake zerbitzariek dauzkaten zerbitzu batzuen exekutagarrietara eta baimen altuekin abiarazten dira. Erasotzaile lokal autentifikatu batek exekutagarri horietako bat programa gaizto batez ordezkatuko balu, hau ere pribilegio altuekin exekutatuko litzateke. Ahultasun horretarako CVE-2018-14787 identifikatzailea erreserbatu da.
- Kakotxen falta bilaketa elementu edo direktorio batean: ISCVren 3.X eta lehenagoko bertsioetan eta Xcelera-ren 4.X eta lehenagoko bertsioetan pribilegio handiekin diharduten Windows zerbitzu batzuk daude. Zerbitzu horiek ez daukate kakotxik beren direktorio definizioan, eta beraz erasotzaile batek zerbitzu horiek ordezka litzake exekutagarriak diren beste batzuengatik. Ahultasun horretarako CVE-2018-14789 identifikatzailea erreserbatu da.

**Etiketak:** Ahultasuna

---

# Hainbat ahultasun Philipsen PageWriter kardiografoetan

**Argitalpen data:** 2018/08/17

**Garrantzia:** Ertaina

**Kaltetutako baliabideak:**

- PageWriter TC10, TC20, TC30, TC50, TC70, 2018ko maiatza baino lehenagoko bertsio guztiak.

**Azalpena:**

Philipsek jakinarazi duenez bere PageWriter kardiografoek hainbat ahultasunen dituzte, sarbide datuen egiaztapen okerraren eta pasahitz barneratuen erakoak. Ahultasun horiek arrakastaz baliatuz gero bufferraren gainezkatzeak eragin litezke edo erasotzaile bat gailuaren ezarpenetan sar liteke eta horiek aldatu.

**Konponbidea:**

Philipsek aurreikusten du 2019. urtearen erdialderako prest izatea ahultasun horiek konpontzen dituen eguneraketa.

Horrez gain, Philipsek ondoko informazioa jakinarazi du dagoeneko fabrikatzaileak zerbitzurik ematen ez dion sistema eragile bati buruz:

- WinCE5 sistema eragile zaharkitua da, fabrikatzaileak dagoeneko ez dio zerbitzurik ematen eta soilik aplikatzen zaie honako gailu hauei: PageWriter TC20, TC30, TC50 y TC70.
- PageWriter TC50 eta TC70k WinCE7 erabil dezakete, eta bezeroaren InCenter-en dago eskuragarri. Sistema eragile zaharkituarekin kezkatuta egonez gero, Philipsek aholkatzen du TC20 eta TC30 gailuak TC50arekin ordezkatzea. 2019. urtearen amaiera alderako eguneraketa bat argitaratuko da TC20 gailurako, sistema eragile bateragarri batera eguneratzeko.

**Xehetasuna:**

- Erabiltzaileak sartutako datuen inolako egiaztapenik ez du egiten PageWriter gailuak. Horren ondorioz bufferraren gainezkatzearen erako ahultasunak edo string formatuko erasoak gerta daitezke. Ahultasun horretarako CVE-2018-14799 kodea erabili da.
- Supererabiltzailearen pasahitz txertatua aurkitzen duen eta sarbide fisikoa duen erasotzaile batek hura erabil lezake gailura sartzeko eta bere konfigurazio guztiak aldatzeko, bai eta dauden pasahitzak berrezartzeko ere. Ahultasun horretarako CVE-2018-14801 identifikatzailea erabili da.

**Etiketak:** Sistema Eragilea, Ahultasuna

# Hainbat ahultasun Yokogawa produktuetan

**Argitalpen data:** 2018/08/17

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- ProSafe-RSrako iDefine, R1.16.3 eta lehenagoko bertsioak.
- STARDOM, VDS R7.50 eta lehenagoko bertsioak, eta FCN/FCJ Simulator R4.20 eta lehenagokoak.
- ASTPLANNER, R15.01 eta lehenagoko bertsioak.
- TriFellows, V5.04 eta lehenagoko bertsioak.
- Yokogawaren 3 geruzako eta 2 geruzako switchak, modelo hauetan:
  - GRVSW-663FA, GRVSW-664FA, GRVSW-665FA, GRVSW-666FA, GRVSW-667FA, GRVSW-660FA, GRVSW-661FA, GRVSW-662FA, GRVSW-668FA, GRVSW-669FA, GRVSW-670FA, GRVSW-671FA, GRVSW-672FA, GRVSW-673FA,
- Hirschmann-en 3 geruzako eta 2 geruzako switchak ere kaltetuak izan dira modelo hauetan:
  - MACH104-20TX-F, MACH104-20TX-FR, MAR1040-4C4C4C4C9999EM9HPY, MAR1040-4C4C4C4C9999EMMHPYY, MAR1040-4C4C4C4C9999ELLHPYY, RS40-0009CCCCEDBPYY, MACH102-8TP-F, MACH102-24TP-F, MAR1040-4C4C4C4C9999EM9HRY1, MAR1040-4C4C4C4C9999EMMHRY1, MAR1040-4C4C4C4C9999ELLHRY1, MAR1040-4C4C4C4C9999EM9HRY2, MAR1040-4C4C4C4C9999EMMHRY2, MAR1040-4C4C4C4C9999ELLHRY2.

**Azalpena:**

Yokogawa fabrikatzaileak hainbat ahultasunen berri eman du lizentzien kudeaketaren funtzioan eta 2 geruza eta 3 geruzako hainbat switchetan. Urruneko erasotzaile batek horiek balia ditzake kode arbitrarioa exekutatzeko edo zerbitzuaren ukapena eragiteko.

**Konponbidea:**

Yokogawak ahultasunak konpontzen dituzten bertsio berriak ditu produktu hauetan:

- ProSafe-RSrako iDefine, R1.16.4 bertsioa
- STARTDOM VDS R8.10
- ASTPLANNER R15.02.01
- TriFellows V5.10

2 geruza eta 3 geruzako switchen kasuan fabrikatzaileak gomendatzen du debug tcpdump komandoa desaktibatzea, ez baitauka firmware berririk.

Informazio gehiagorako erreferentziazko lotura ikusi edo harremanetan jarri fabrikatzailearen laguntza ekipoarekin.

**Xehetasuna:**

- Kaltetutako Yokogawa produktuen lizentzien kudeaketaren funtzioa ez dago modu zuzenean ezarria. Horrek erasotzaile bati ahalbidetuko lioke bereziki diseinatutako paketeak baliatzea bufferraren gainezkatzea eragiteko, eta horrela zerbitzuaren ukapena eragingo luke edo urrunetik kodea exekuta lezake.
- 2 geruza eta 3 geruzako Vnet/IP switchen debug funtzioak ahultasun bat dauka tcpdump komandoan. Debug kontsolan tcpdump komandoa exekutatzen den bitartean erasotzaile batek ahultasuna balia lezake komunikazioen deskonexioa eragiteko edo haietan interferitzeko.

**Etiketak:** Eguneraketa, Ahultasuna

# Hainbat ahultasun Emerson-en DeltaV DCS Workstations-en

**Argitalpen data:** 2018/08/17

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- DeltaV, v11.3.1, v12.3.1, v13.3.0, v13.3.1 eta R5 bertsioak

**Azalpena:**

Nozomi Networkseko Younes Dragonik, CyberXeko Ori Perezek eta Emersonek eman dute ahultasun hauen berri. Horiek arrakastaz baliatuz gero erasotzaile batek kode arbitrarioa exekuta lezake eta malwarea injekta eta zabal lezake lan estazioen artean.

**Konponbidea:**

Emersonek erabiltzaileei aholkatzen die partxeak aplikatzea kaltetutako produktuei. Emersonen Guardianen Laguntza atarira sarbidea duten erabiltzaileentzat software partxeak eskuragarri daude lotura honetan: https://guardian.emersonprocess.com/. Informazio gehiago eskuratzeko Emersonek ondoko artikulua gomendatzen du: Knowledge Base AK-1800- 0042 (DSN18003).

CVE-2018-14797, CVE-2018-14795 eta CVE-2018-14791 ahultasunak ezin dira baliatu zerrenda zuriko neurriak hartzen badira, fitxategiak ezingo bailirateke gainidatzi.

Ahultasun hauen eta beste batzuen aurreko arriskua murrizteko DeltaV sistemak eta erlazionatutako osagaiak ezartzea eta konfiguratzea gomendatzen da, DeltaVren Segurtasun eskuliburuan azaltzen den moduan, Emersonen Guardianen Laguntza atarian eskuragarri dagoena.

**Xehetasuna:**

- Bereziki diseinatutako DLL fitxategi bat bilaketa bidean jar daiteke eta barneko DLL baliozko baten modura kargatu. Horrek kode arbitrarioa exekutatzea ahalbidetu dezake. Ahultasun horretarako CVE-2018-14797 identifikatzailea erabili da.
- Bidearen egiaztapen oker bat baliatuz erasotzaile batek fitxategi exekutagarriak ordezka litzake. Ahultasun horretarako CVE-2018-14795 identifikatzailea erabili da.

- Administrazio pribilegiorik gabeko erabiltzaileak gai dira kaltetutako produktuetan exekutagarriak eta liburutegiak aldatzeko. Ahultasun horretarako CVE-2018-14791 identifikatzailea erabili da.
- Irekita dagoen komunikazio ataka bat baliatua izan daiteke kode arbitrarioa exekutatzeko. Ahultasun horretarako CVE-2018-14793 identifikatzailea erabili da.

**Etiketak:** Eguneraketa, Malware, Ahultasuna

---

# Hainbat ahultasun Tridium-en Niagara-n

**Argitalpen data:** 2018/08/17

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- Niagara AX Framework, 3.8 eta lehenagoko bertsioak
- Niagara 4 Framework, 4.4 eta lehenagoko bertsioak

**Azalpena:**

Johnathan Gains eta Leet Cyber Security-k ahultasun hauen berri eman dute, direktorioaren jauzi eta autentifikazio oker erakoak. Ahultasun horiek arrakastaz baliatuz gero, sartzea lortu den gailua blokea liteke eta bufferraren gainezkatzearen egoera batek urrunetik kodea exekutatzea ahalbidetu lezake.

**Konponbidea:**

Tridiumek ondoko neurriak hartzea aholkatzen du:

- Niagara AX v3.8: 4 (3.08.401) eguneraketa aplikatzea
- Niagara 4 Framework v4.4: 1 (4.4.92.2.1) eguneraketa aplikatzea

Eguneraketei buruzko informazio gehiago lotura honetan aurki daiteke:

https://www.tridium.com/~/media/tridium/library/documents/niagara_ax_38_update_4niagara_44_update_1.ashx?la=en

**Xehetasuna:**

- Microsoft Windows sistemetan instalatutako Tridium Niagara AX eta Niagara 4 sistemek duten direktorioaren jauzi erako ahultasun bat balia daiteke plataformaren administratzaile kredentzial baliozkoak erabiliz. Ahultasun horretarako CVE-2017-16744 identifikatzailea erabili da.
- Erasotzaile batek Niagararen plataforma lokalean saioa has dezake desgaitutako kontu izen bat erabiliz eta pasahitza hutsik utziz. Horrela Niagararen sistemara administratzaile sarbidea lortuko luke. Ahultasun horretarako CVE-2017-16748 identifikatzailea erabili da.

**Etiketak:** Eguneraketa, Ahultasuna

---

# Eltex-en ESP-200 routerrean hainbat ahultasun

**Argitalpen data:** 2018/08/20

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- ESP-200 routerra, 1.2.0 bertsioa

**Azalpena:**

Kaspersky Lab ICS-CERTeko Alexander Nochvay eta Andrey Muravitsky-k hainbat eratako ahultasun batzuen berri eman dute: komandoen injekzioa, konfigurazio ez-seguruak, pasahitz lehenetsiak eta informazioaren hedapena. Ahultasun horiek arrakastaz baliatuz gero erasotzaile batek hainbat ekintza egin litzake: pribilegioen eskalatzea, kode arbitrarioa exekutatzea, erasoaren azalera zabaltzea edo informazioa hedatzea.

**Konponbidea:**

- Firmwarearen 1.3.0 bertsiora eguneratzea gomendatzen da.

**Xehetasuna:**

- Lehenetsitako pasahitzak erabiliz, autentifikaziorik gabeko erasotzaile batek administratzaile saioa has lezake gailuan. Ahultasun horretarako CVE-2018-15360 identifikatzailea erabili da.
- Pribilegio baxuekin autentifikatutako erasotzaile batek sudoren konfigurazio ez-seguru bat balia lezake erasoaren azalera zabaltzeko. Ahultasun horretarako CVE-2018-15359 identifikatzailea erabili da.
- Pribilegio baxuekin autentifikatutako erasotzaile batek pribilegio altuko erabiltzaile bat aktiba lezake eta erasoaren azalera handitzeko erabili. Ahultasun horretarako CVE-2018-15358 identifikatzailea erabili da.
- Pribilegio baxuekin autentifikatutako erasotzaile batek informazioa eskura lezake erabiltzaile bakoitzaren pasahitza dagoen hashetik. Ahultasun horretarako CVE-2018-15357 identifikatzailea erabili da.
- Autentifikatutako erasotzaile batek kode arbitrarioa exekuta lezake komandoen injekzioaren bidez. Ahultasun horretarako CVE-2018-15356 identifikatzailea erabili da.

**Etiketak:** Eguneraketa, Ahultasuna

---

# Kraftway-ren Kraftway-24F2XG routerrean hainbat ahultasun

**Argitalpen data:** 2018/08/20

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- Kraftway-24F2XG, firmwarearen 3.5.30.1118 bertsioa

**Azalpena:**

Kaspersky Lab ICS CERTeko Alexander Nochvay eta Andrey Muravitsky ikertzaileek era ezberdineko ahultasunen berri eman dute: zerbitzuaren ukapena, SSL zifratu ahula, bufferraren gainezkatzea eta kredentzialak lehenetsita. Ahultasun horiei esker, urruneko erasotzaile batek zerbitzuaren ukapena eragin lezake, routerrera sartzeko pribilegioak lortu, urrunetik kode gaiztoa exekutatu edo eskualdatutako informazioa deszifratu.

**Konponbidea:**

- Firmwarearen 3.5.47-315-gef7 eta goragoko bertsioetara eguneratzea gomendatzen da.

**Xehetasuna:**

- Kaltetutako gailuan autentifikatu gabeko urruneko erasotzaile batek administratzaile pribilegioak eskura litzake routerrera sartzeko lehenetsitako kredentzialak erabiliz. Ahultasun horretarako CVE-2018-15350 identifikatzailea erabili da.
- Urruneko erasotzaile batek lotura gaizto bat sor lezake eta kaltetutako routerraren barnean pribilegioak dituen erabiltzaile bati (biktima) bidali, zerbitzuaren ukapena sortzeko. Ahultasun horretarako CVE-2018-15351 identifikatzailea erabili da.
- Pribilegio gutxi dituen urruneko erasotzaile batek kaltetutako gailuan zerbitzuaren ukapena eragin lezake. Ahultasun horretarako CVE-2018-15352 identifikatzailea erabili da.
- Web interfazeak bufferraren gainezkatzearen bi ahultasun ditu. Horiek baliatuz erasotzaile batek zerbitzuaren ukapena eragin lezake edo urruneko kodea exekutatu. Ahultasun horietarako CVE-2018-15353 eta CVE-2018-15354 identifikatzaileak erabili dira.
- SSLren 2 eta 3 bertsioek komunikazioek duten zifratuaren sendotasunarekin zerikusia duten ahultasunak dituzte. Erasotzaile batek ahultasun hori balia lezake eskualdatutako informazioa deszifratzeko Man-in-the-Middle bezalako eraso teknikak erabiliz. Ahultasun horretarako CVE-2018-15355 identifikatzailea erabili da.

**Etiketak:** Komunikazioak, Pribatutasuna, Ahultasuna

---

# Philipsen IntelliVue Information Center iX-n baliabideen kontrolik gabeko kontsumoa

**Argitalpen data:** 2018/08/22

**Garrantzia:** Ertaina

**Kaltetutako baliabideak:**

- Philips IntelliVue Information Center iX, B.02 bertsioa

**Azalpena:**

Erabiltzaile anonimo batek eman du baliabideen kontrolik gabeko kontsumo erako ahultasun honen berri. Hori arrakastaz baliatuz gero, zerbitzuaren ukapen egoera eragin liteke, eta sistema eragileak erantzuteari utziko lioke sare erasoaren ondorioz. Aurreikusitako erabilera betetzeko aplikazioek daukaten gaitasunari eragingo lioke horrek.

**Konponbidea:**

- Philipsek arintzeak identifikatu eta ezarri ditu ahultasun hau baliatzeko arriskua murriztearren. 2018ko irailaren amaieran partxea eskuragarri jartzen den bitartean, kaltetutako gailuen erabiltzaileek ahultasun honen arriskua arintzearren, konpainiak aholkatzen du erabilera argibideak eta zerbitzu gidak jarraitzea, konpentsazio kontrolak eskaintzen baitituzte.

**Xehetasuna:**

- Erasotzaile batek gailuaren eskuragarritasuna arriskuan jar lezake hasierako UDP eskaera ugari bidaliz. Ahultasun horretarako CVE-1999-0103 identifikatzailea erabili da.

**Etiketak:** Ahultasuna

---

# Becton, Dickinson and Company-ren (BD) Alaris Plus-en autentifikazio ezegokia

**Argitalpen data:** 2018/08/24

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:** Alaris Plus osasun xiringaren bonben ondoko bertsioak, 2.3.6 bertsioa eta aurrekoak hain zuzen, kaltetuta daude:

- Alaris GS
- Alaris GH
- Alaris CC
- Alaris TIVA

**Azalpena:**

CyberMDXeko Elad Luz ikertzaileak BD fabrikatzaileri eman dio ahultasun honen berri, eta fabrikatzailea harremanetan jarri da ICS-CERTekin (NCICC). Ahultasunak zerikusia du autentifikazio ezegokiarekin, eta horrek erasotzaile bati baimenik gabe gailura sartzea ahalbidetuko lioke. Horrela bere jardunean eragin lezake serieko ataka baten bidez zerbitzari batera konektatuta dagoenean.

**Konponbidea:**

Fabrikatzaileak jakinarazi du ahultasuna ezin dela baliatu gailua Alaris Gateway lan estazio batera konektatuta badago. Gainera, erasotzaileak ahultasuna baliatuz ezingo luke urrunetik gailura sartu, ezta PHI edota PIIra ere.

Ahultasun honi lotutako arriskuak gutxitzearren, BDk aholkatzen du hurrengo arintze eta kontrol neurri konpentsatzaileak jarraitzea:

- Erasoak zerbitzarien terminalek duten ahultasun ezagun bat baliatzen du. Terminal horiek erabiltzen dituzten erabiltzaileek ulertu behar dute zerbitzarien terminalen erabilpena ez dela bateragarria.
- Erabiltzaileek ziurtatu behar dute kaltetutako gailuekin segmentatutako sare inguru batean ari direla lanean, edo edozein saretatik isolatutako gailu batekin ari direla, bere jardunean eraginik izango ez duen inolako komunikazio motarik gabe.
- Erabiltzaileek Alaris Gateway lan estazioaren bitartezko konexioak erabili behar dituzte. Egoera honek urruneko kontrolaren funtzioa desaktibatuko luke, eta horrela ahultasuna ezingo litzateke baliatu.

**Xehetasuna:**

- Erabiltzaileen identifikazioa behar duten funtzionalitateetarako autentifikazio ezegokia. Ahultasun horretarako CVE-2018-14786 identifikatzailea erabili da.

**Etiketak:** Ahultasuna

---

# Schneider Electric-en PowerLogic PM5560en Cross Site Scripting erako ahultasuna

**Argitalpen data:** 2018/08/24

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- PM5560, firmwarearen 2.5.4 bertsioa baino lehenagokoak

**Azalpena:**

Ezequiel Fernandezek eta Bertin Josek cross protocol inyection erako ahultasun honen berri eman dute. PowerLogic PM5560 produktuaren barneratutako web zerbitzariari eragiten dio, eta javascript kodea exekutatzea ahalbidetu lezake.

**Konponbidea:**

- Ondoko eguneraketa aplikatzea: https://www.schneider-electric.com/en/download/document/PM5560_PM5563_V2.5.4_Release/

**Xehetasuna:**

- PowerLogic PM5560 produktuaren barneratutako web zerbitzariak cross site scripting erako erasoa jasan lezake. Urruneko erasotzaile batek ahultasun hori balia lezake, sarrera datuak web bidez manipulatuz, javascript kodea exekutatzea lortzeko. Ahultasun horretarako CVE-2018-7795 identifikatzailea erabili da.

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

---

# Scheiner Electric-en Modicon M221en baldintza ezohikoen egiaztapen ezegokia

**Argitalpen data:** 2018/08/27

**Garrantzia:** Ertaina

**Kaltetutako baliabideak:**

- Modicon M221, V1.6.2.0 firmwarearen aurreko bertsio guztiak.

**Azalpena:**

Radifloweko Yehonatan Kfir-ek Schneider Electric-i eman dio Modicon M221 produktuei eragiten dien ahultasun baten berri, salbuespenezko edo ezohiko baldintzen egiaztapen ezegoki bat alegia. Urruneko erasotzaile batek kaltetutako gailuak berrabiaraz litzake.

**Konponbidea:**

Schneider Electricek partxe bat garatu du ahultasun honetarako, eta firmwarearen V1.6.2.0 bertsioan sartu du, SoMachine Basic V1.6 SP2rekin banatzen dena. Ondoko loturatik jaits daiteke: https://www.schneider-electric.com/en/download/document/SoMachineBasicV1.6SP2/

**Xehetasuna:**

Urruneko erasotzaile batek gaizki sortutako programazio protokoloen tramak bidal litzake, kaltetutako gailuak berrabiaraztea eragin lezaketenak, salbuespeneko edo ezohiko baldintzen egiaztapen ezegoki baten ondorioz. Ahultasun horretarako CVE-2018-7789 identifikatzailea erreserbatu da.

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

---

# Autentifikazioari ihes egitea Echelon-en i.LON 600en

**Argitalpen data:** 2018/08/28

**Garrantzia:** Txikia

**Kaltetutako baliabideak:**

- i.LON 600 produktu guztiak

**Azalpena:**

Maxim Rupp ikertzaile independenteak Echelonen i.LON 600 produktuek duten autentifikazioaren ihes erako ahultasun honen berri eman du. Urruneko erasotzaile batek autentifikazioa saihets lezake eta konfigurazioaren informazioa eta errendimendu estatistikak irakurri.

**Konponbidea:**

- Mehatxuen aurreko arriskua murriztearren, Echelonek gomendatzen du suebaki baten atzean instalatzea i.LON 600 gailuak eta horiek erabiltzen dituen edozein zerbitzari, edo bestela gailu gehiagorik gabeko VLAN batean. VLAN erabiliz, i.LON 600 eta lotutako zerbitzarien sistema bereko parte ez diren beste barne gailu batzuen eta erabiltzaileen mehatxua murriztea lortzen da. Suebaki bat erabiltzen denean, eta mehatxuen aurreko arriskua murriztearren, Echelonek gomendatzen du suebakiak ataken inolako birbidalketarik ez egitea i.LON 600era.

**Xehetasuna:**

- i.LON 600en autentifikazioa WebParams.dat fitxategiko konfigurazio jarraibideek kontrolatuta dago. Fitxategi edo direktorio multzo jakin bat autentifikaziorik gabe eskuragarria ez litzatekeela izan behar zehazterakoan, bidea konfigurazio fitxategian kate baten modura jartzen da, eta karaktere komodin aukerakoak (*) izan ditzake, zero karaktere edo gehiago kointzidiarazteko. Web eskari bat egiten denean, URIak bat etorri behar du emandako bide osoarekin, edo bestela ez da autentifikaziorik eskatuko. URIan barra gainjarriak dituzten web eskariak bidaltzerakoan (adibidez, ?/forms/////Echelon/SetupSecurity.htm?), bidea ez da bat etorriko autentifikazioa eskatzeko konfiguratutakoarekin, eta hartara sarbidea lortuko da inolako erabiltzaile izenik eta pasahitzik gabe.

**Etiketak:** Ahultasuna

---

# Hainbat ahultasun Schneider Electric-en Modicon M221-en

**Argitalpen data:** 2018/08/29

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- Modicon M221, V1.6.2.0 bertsioa baino lehenagoko guztiak

**Azalpena:**

New Orleanseko Unibertsitateko Irfan Ahmed, Hyunguk Yoo, Sushma Kalle eta Nehal Ameen ikertzaileek Schneider Electric-en Modicon M221 produktuei eragiten dieten hainbat ahultasunen berri eman dute. Era hauetakoak dira: informazioaren kudeaketan akatsa, eta baimen, pribilegio eta sarbide kontrolaren kudeaketa okerra. Urruneko erasotzaile batek pasahitzak berridatz edo deskodetu litzake edo autentifikazio sekuentzia birbidali.

**Konponbidea:**

- Schneider Electric-ek partxe bat garatu du ahultasun honetarako, eta firmwarearen V1.6.2.0 bertsioan sartu du, SoMachine Basic V1.6 SP2rekin banatzen dena. Ondoko loturatik jaits daiteke: https://www.schneider-electric.com/en/download/document/SoMachineBasicV1.6SP2/

**Xehetasuna:**

- Baimenik gabeko erabiltzaile bati autentifikazio sekuentziak birbidal ditzan ahalbidetzen dion ahultasuna. Erasotzaile bat kaltetutako produktura konekta liteke eta PLCren programa originala igotzea lor lezake. Ahultasun horretarako CVE-2018-7790 identifikatzailea erreserbatu da.
- Baimenik gabeko erabiltzaileei pasahitz originala gainidaztea ahalbidetzen dien ahultasuna. Erasotzaile batek PLCren programa originala igotzea lor lezake. Ahultasun horretarako CVE-2018-7791 identifikatzailea erreserbatu da.
- Rainbow taulak erabiliz baimenik gabeko erabiltzaileei pasahitzak deskodetzea ahalbidetzen dien ahultasuna. Ahultasun horretarako CVE-2018-7792 identifikatzailea erreserbatu da.

**Etiketak:** Schneider Electric, Ahultasuna

---

# Kodearen ahultasuna Qualcomm Life-ren Capsule Datacaptor Terminal Server-en

**Argitalpen data:** 2018/08/29

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

Capsule Datacaptor Terminal Server-en (DTS) ondoko bertsioak osasun gailu baten informazio sistema bateko parte dira eta kaltetuta daude:

· Allegro RomPager barneratutako web zerbitzarian dauden Capsule DTSren bertsio guztiak, 4.01etik 4.34ra bitartean.

**Azalpena:**

CyberMDXeko Elad Luz-ek kodearen ahultasun erako ahultasun honen berri eman du. Ahultasun hori arrakastaz baliatuz gero urruneko erasotzaile batek kodea exekuta lezake baimenik gabe, gailuan administratzaile pribilegioak eskuratzearren.

**Konponbidea:**

Capsule Technologies-ek DTSren Single Board bertsioan ahultasuna konpontzen duen firmwarearen eguneraketa bat argitaratu du, originalki 2009an kaleratua. Capsule Technologies-ek arren eskatzen die DTSren Single Board bertsioa duten erabiltzaile guztiei Capsule-ren bezeroaren webgunetik firmwarea deskarga dezaten eta kaltetutako gailuetan ezar dezaten partxeatze prozedura jarraituz. Bezeroaren webgunerako sarbidea hemen aurki daiteke:
https://customers.capsuletech.com/

Arazo teknikoak direla-eta firmwarearen eguneraketak ahultasuna soilik konpontzen du Single Board bertsioetan, eta ez beste hauetan:

- Dual Board
- Capsule Digi Connect ES converted to DTS
- Capsule Digi Connect

Capsulek hiru DTS bertsioetakoren bat duten erabiltzaileei gomendatzen die barneratutako web zerbitzaria desgaitzea ahultasun honen eragina arintzearren. Web zerbitzaria soilik erabiltzen da hasierako ezarpenaren konfiguraziorako, eta ez da beharrezkoa gailuaren urruneko laguntza tekniko iraunkorrerako.

**Xehetasuna:**

Ahultasun hau baliatuz erasotzaile batek HTTP cookie bat bidal lezake web administrazioaren atarira, gailuaren memorian datu arbitrarioak idazteko. Horrekin urrunetik kodea exekutatu ahal izatea gaitu liteke. Ahultasun horretarako CVE-2014-9222 identifikatzailea erabili da.

**Etiketak:** Eguneraketa, Ahultasuna

---

# Hainbat ahultasun Philips-en e-Alert Unit-en

**Argitalpen data:** 2018/08/31

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- Philips e-Alert, R2.1 eta lehenagoko bertsioak

**Azalpena:**

Philipsek hainbat ahultasun aurkitu ditu. Azpisare berean dagoen erasotzaile batek horiek arrakastaz baliatuz gero, erabiltzailearen kontakturako xehetasunak eta kaltetutako produktuen integritatea edota eskuragarritasuna kaltetu edo arriskuan jar litezke. Ahultasun horiei esker erasotzaile batek aplikazioan ustekabeko sarrera datuak sar litzake, kode arbitrarioa exekutatu, unitatearen informazioa eskuratu edo kaltetutako unitateek funtzionatzeari utz diezaioten lor lezake.

**Konponbidea:**

2018ko ekainean Philipsek ahultasun horietako batzuk konpontzen zituen R2.1 bertsioa argitaratu zuen. Gainerako ahultasunen kasuan, Philipsek beste software eguneraketa bat aurreikusia dauka 2018ko amaierarako.
Philipsek zerbitzu aukeren berri emango die kaltetutako erabiltzaile guztiei. Era berean, bere produktuek duten segurtasun webgunea bisitatzea aholkatzen du, gai honi buruz eta Philipsen beste produktu batzuei buruz argitaratuta dagoen segurtasun informazio berriena eskuratzearren. Informazioa ondoko loturan dago eskuragarri:
https://www.philips.com/productsecurity
LANeko ahultasunen aurrean berehalako arintze modura, eta eguneraketa aplika daitekeen bitartean, Philipsek ondokoa gomendatzen die erabiltzaileei:

- Sareko segurtasuneko praktika onak ezartzen direla bermatzea.
- e-Alert-en sarerako sarbidea murriztea, produktuaren dokumentazioak dioenaren arabera.

e-Alert-eko beren instalazio bereziei buruz galderak dituzten erabiltzaileek Philipsen laguntza zerbitzu lokalarekin edo e-Alert-eko eskualdeko laguntza zerbitzuarekin harremanetan jarri behar dira. Harremanetarako informazioa hemen eskura daiteke:

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

**Xehetasuna:**

- Sarrera datuak oker balioztatzea: softwareak ez du sarrera-datuen balioztatze zuzenik egiten, eta hori baliatuz erasotzaileak sarrera-datuak eman litzake aplikazioaren gainerakoak espero ez duen modu batean. Horren ondorioz unitatearen zati batzuek nahi gabeko sarrera bat jasoko lukete, eta horrek kontrol fluxu aldatua, baliabide baten kontrol arbitrarioa edo kode arbitrarioaren exekuzioa eragin lezake. Ahultasun horretarako CVE-2018-8850 identifikatzailea erabili da.
- Cross Site Scripting (XSS): softwareak ez ditu modu egokian iragazten sarrera parametroak. Horri esker erasotzaile batek kodea exekuta lezake bezeroaren aldean biktima bat web zerbitzarira bere nabigatzailearen bidez sartzen denean. Ahultasun horretarako CVE-2018-8846 identifikatzailea erabili da.
- Lehenetsitako baimen okerrak: Softwarea instalatzerakoan objektu batentzat baimen okerrak ezartzen ditu, eta horrek objektua agerian uzten du nahi gabeko erabiltzaile baten aurrean. Ahultasun horretarako CVE-2018-8848 identifikatzailea erabili da.
- Informazio sentikorraren transmisioa testu lauan: softwareak informazio sentikorra edo segurtasun kritikoko informazioa testu lauan transmititzen du, erasotzaile batek atzeman dezakeen komunikazio bide baten bidez. Produktuaren komunikazio kanala ez dago zifratuta, eta horren ondorioz kontaktu pertsonalerako informazioa eta sare beraren barnean aplikazioaren saio hasierako kredentzialak zabal litezke. Ahultasun horretarako CVE-2018-8842 identifikatzailea erabili da.
- Baliabideen kontrolik gabeko kontsumoa: softwareak ez du modu egokian murrizten erabiltzaile batek eskatzen duen baliabideen tamaina edo kopurua. Hori erabil liteke aurreikusitakoak baino baliabide gehiago kontsumitzeko. Ahultasun horretarako CVE-2018-8854 identifikatzailea erabili da.
- Pasahitz barneratuen erabilpena: softwareak barneratuta dauka barneko datuak zifratzeko erabiltzen den giltza kriptografikoa. Ahultasun horretarako CVE-2018-8856 identifikatzailea erabili da.

Ahultasun horiez gain, kritikotasun txikiagoko beste batzuk ere aurkitu dira. Horietarako ondoko identifikatzaileak erreserbatu dira: CVE-2018-14803, CVE-2018-8844, CVE-2018-8852.

**Etiketak:** Ahultasuna