2018ko Uztailaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Siemens-en SICLOCK TC gailuetan hainbat ahultasun

Argitalpen data: 2018/07/04

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SICLOCK TC100, bertsio guztiak.
- SICLOCK TC400, bertsio guztiak.

Azalpena:

Siemensek SICLOCK TC gailuekin zerikusia duten hainbat ahultasun antzeman ditu. Horien bitartez urruneko erasotzaile batek zerbitzuaren ukazioak eragin litzake, autentifikazioari ihes egin liezaioke, kode arbitrarioa exekutatu lezake eta firmwarea aldatu ahal izango luke, bai gailuarena eta bai horren administrazioa ahalbidetzen duen bezeroarena ere.

Konponbidea:

Siemensek ondoko urratsak egitea gomendatzen die bere bezeroei, ahultasunak murrizteko eta arriskua gutxitzeko:

- Denbora iturri erredundanteak erabiltzea eta horien egiaztapen bat egitea, denboraren informazioaren kontrola izatearren.
- Gailuak dauden sarera sartzeko sarbidea suebakiekin babestea, agerian egoteko arriskua murriztearren.
- Ataka guztiak filtratzea gomendatzen da, denboraren sinkronizaziorako beharrezkoak direnak salbu.
  - Denboraren sinkronizazioa NTP protokoloaren bidez egiten bada, suebakian 123/UDP ataka ireki behako litzateke.
  - SIMATIC denbora sinkronizazioa erabiliz egiten bada, suebakian 22223/UDP eta 22224/UDP atakak ireki beharko lirateke.
- Parametro hauek konfiguratzeko SICLOCK TC gailuarekin zuzeneko konexio bat erabiltzea aholkatzen da.
- Defentsa Sakona kontzeptua aplikatzea: https://www.siemens.com/cert/operational-guidelines-industrial-security

Xehetasuna:

- Zerbitzua ukatzea: Gailura sarbidea duen urruneko erasotzaile batek zerbitzuaren ukazio egoera eragin lezake gailura pakete jakin batzuk bidalita, eta horren ondorioz, berrabiatzeak gertatuko lirateke eta kaltetutako gailuaren funtzionaltasunean eragingo luke. Funtzionaltasuna berreskuratzen da GPS edo NTP bidez denboraren sinkronizazioa osatzen denean. Ahultasun horretarako CVE-2018-4851 identifikatzailea erreserbatu da.
- Autentifikazioari ihes egitea: Urrutiko erasotzaile batek autentifikazioari ihes egin liezaioke erasotzen ari den gailuari buruzko aski ezagutza badu. Ahultasun hau arrakastaz baliatuz gero gailuaren konfigurazioa irakur eta alda liteke. Ahultasun horretarako CVE-2018-4852 identifikatzailea erreserbatu da.
- Kode arbitrarioa exekutatzea: 69/UDP atakara sarbidea duen urruneko erasotzaile batek gailuaren firmwarea alda lezake eta kode arbitrarioa exekutatzea lortu. Ahultasun hau baliatzeko ez da beharrezkoa erabiltzailearen interakzioa. Ahultasun horretarako CVE-2018-4853 identifikatzailea erreserbatu da.
- Kode arbitrarioa exekutatzea: 69/UDP atakara sarbidea duen urruneko erasotzaile batek gailuan gordeta dagoen bezero administratzailea alda lezake. Egiazko erabiltzaile batek aldatutako bezeroa jaitsi eta exekutatzen badu, erasotzaileak bezeroaren sisteman kodea exekutatzea lor lezake. Ahultasun horretarako CVE-2018-4854 identifikatzailea erreserbatu da.

Gainerako ahultasunetarako honako identifikatzaileak erreserbatu dira: CVE-2018-4855 eta CVE-2018-4856.

Etiketak: Siemens, Ahultasuna

Hainbat ahultasun Rockwell Automation-en Allen-Bradley Stratix 5950en

Argitalpen data: 2018/07/04

Garrantzia: Handia

Kaltetutako baliabideak:

Allen-Bradley Stratix 5950 gailuek Cisco Systems-en Adaptive Security Appliance (ASA) erabiltzen dute sistema eragile nagusi modura. Ciscok hainbat jakinarazpen argitaratu ditu ASA softwareak dituen ahultasun batzuei buruz. Cisco ASAren 9.6.2 bertsioa eta lehenagokoak erabiltzen dituzten Allen-Bradley Stratix 5950 gailu hauek daude eraginda:

- 1783-SAD4T0SBK9
- 1783-SAD4T0SPK9
- 1783-SAD2T2SBK9
- 1783-SAD2T2SPK9

Azalpena:

Rockwell Automationek balioztatze desegokiko hainbat ahultasun antzeman ditu. Ahultasun horiek modu arrakastatsuan baliatuz gero, erasotzaile batek bezeroaren egiaztapena saihestu lezake kaltetutako gailurako konexioak sortzeko edo gailua blokeatzea eragiteko.

Konponbidea:

Rockwell Automationek erabiltzaileak informatuko ditu firmwarearen eguneraketa eskuragarri egon bezain azkar. Eguneraketak argitaratzen diren bitartean, kaltetutako produktuak dituzten erabiltzaileei ondoko estrategiak jarraitzea gomendatzen die, arriskuak gutxitzearren:

- CVE-2018-0228 ? ASA eta FTD konfigurazio komandoak konfiguratu egin daitezke baimendutako konexio eskaeren kopurua mugatzeko. Konfigurazio parametro horiek erabiltzeak konexio kopurua murriztu dezake eta DoS erasoaren eragina neurri handi batean gutxitu.
- CVE-2018-0227 ? Ez dago konponbiderik eskuragarri.
- CVE-2018-0231 ? Ez dago konponbiderik eskuragarri.
- CVE-2018-0240 ? Ez dago konponbiderik eskuragarri.
- CVE-2018-0296 ? Ciscok snort arau bat argitaratu du IDSn erabil daitekeena babesteko. https://www.cisco.com/web/software/286271056/117258/sf-rules-2018-06-07-new.html

Xehetasuna:

- Sarbide datuak oker balioztatzea: Sarbide fluxuaren sorkuntzaren funtzionaltasunean Cisco ASAren ahultasun batek ahalbidetu lezake autentifikatu gabeko urruneko erabiltzaile batek CPUaren %100erainoko erabilpena eragitea, zerbitzuaren ukazio egoera (DoS) sortuz. Ahultasun horretarako CVE-2018-0228 identifikatzailea erabili da.
- Ziurtagiriaren balioztatze okerra: Cisco ASAren Bezeroaren Ziurtagiriaren Autentifikazioaren funtzioaren ahultasun batek ahalbidetu lezake autentifikatu gabeko urruneko erasotzaile batek SSL VPN konexio bat sortzea eta SSL ziurtagiriaren egiaztatze pausoak saihestea. Ahultasun horretarako CVE-2018-0227 identifikatzailea erabili da.
- Sarbide datuak oker balioztatzea: Cisco ASA eta Cisco Firepower Threat Defense (FTD) softwarearen Garraio Geruzako Segurtasun liburutegiaren ahultasun batek ahalbidetu lezake autentifikatu gabeko urruneko erasotzaile batek birkarga bat eragitea kaltetutako gailuan, zerbitzuaren ukazio egoera (DoS) sortuz. Ahultasun horretarako CVE-2018-0231 identifikatzailea erabili da.
- Baliabideen administrazio akatsak: Cisco ASA eta Cisco FTD softwarearen aplikazio geruzaren protokolo ikuskaritzaren funtzioak dituen hainbat ahultasunek ahalbidetu lezakete autentifikatu gabeko urruneko erasotzaile batek birkarga bat eragitea kaltetutako gailuan, zerbitzuaren ukazio egoera (DoS) sortuz. Ahultasun horretarako CVE-2018-0240 identifikatzailea erabili da.
- Sarbide datuak oker balioztatzea: Cisco ASAren web interfazeak duen ahultasun batek ahalbidetu lezake autentifikatu gabeko urruneko erasotzaile batek birkarga bat eragitea kaltetutako gailuan, zerbitzuaren ukazio egoera (DoS) sortuz. Era berean, softwarearen hainbat bertsiotan gerta liteke ASA ez birkargatzea, eta horrela informazio sentikorra eskura liteke direktorio jauziaren bidez. Ahultasun horretarako CVE-2018-0296 identifikatzailea erabili da.

Etiketak: Cisco, Ahultasuna

Sarrera datuen egiaztapen okerra ABBren Panel Builder 800en

Argitalpen data: 2018/07/09

Garrantzia: Handia

Kaltetutako baliabideak:

- Panel Builder 800en bertsio guztiak

Azalpena:

Leahy Center for Digital Investigation-eko Michael DePlante ikertzaileak eta Trend Microko Michael Flandersek, biak Trend Microko Zero Day Initiativerekin lankidetzan, sarrera datuen egiaztapen okerreko ahultasun bat aurkitu dute. Erasotzaile batek ahultasun hori balia lezake kode arbitrarioa sartu eta exekutatzeko.

Konponbidea:

Une honetan ABB ahultasun hau ikertzen ari da, erabiltzaileei babes egokia eskaintzearren. Arazoa etorkizuneko bertsioetan konponduko da. Nolanahi ere, kaltetutako produktuen eguneraketak eskuragarri jarri bitartean, fabrikatzaileak adierazitako arintze neurriak jarraitzea aholkatzen da.
Gomendatutako segurtasun praktikek eta firewallaren konfigurazioek prozesuen kontrol sare bat babesten lagun dezakete saretik kanpora sortzen diren erasoetatik. Praktika horietako batzuk honakoak dira:

- Panel Builder 800en erabiltzaileen zibersegurtasunarekiko kontzientziazioa areagotzea:
  - Kontrol industrialeko sistemetarako zibersegurtasun praktika onenen aholku orokorrak azalduz.
  - Panel Builder malwarearekin infektatzea posible dela informatuz.
  - Ustekabean edota jatorri ezezagunetik jasotzen diren fitxategiekin kontuz ibiltzearen garrantzia azalduz.
- Transferitutako fitxategiak arretaz ikuskatu, birusen kontrako software eguneratu batekin eskaneatzea barne, horrela soilik legitimoak diren fitxategiak transferitu daitezen.
- Erabiltzaileen kontuak kudeatzea autentifikazio egokia erabiliz eta baimenak kudeatzea pribilegio minimoaren printzipioa erabiliz.

Xehetasuna:

Erasotzaile batek ohartarazpen honetan azaldutako ahultasuna balia lezake, erabiltzaile bat engainatuz bereziki diseinatutako fitxategi bat ireki dezan. Horrela, erasotzaileak kode arbitrarioa sartzea edo exekutatzea lor lezake. Kontuan izan behar da ahultasun hau ezin dela urrunetik baliatu eta ezta erabiltzailearen interakziorik gabe ere.

Etiketak: Ahultasuna

Kodearen urrutiko exekuzioa Pepperl Fuchs produktuetan

Argitaratze-data: 2018/07/09

Garrantzia: Handia

Kaltetutako baliabideak:

- VisuNet RM, VisuNet PC eta Box Thin Client BTC familien produktu guztiak.

Azalpena:

Preempt eta Research Labs enpresetako Eyal Karni, Yaron Zinar eta Roman Blachman segurtasun ikertzaileek urrutiko exekuzio motako ahultasun bat antzeman dute Microsoften Credential Security Support Provider (CredSSP) protokoloan. Erasotzaile batek ahultasun hori baliatu lezake erabiltzaile kredentzialak eman eta xede sisteman kode arbitrarioa exekutatzeko.

Konponbidea:

- RM Shell 4 exekutatzen ari diren Pepperl Fuchs HMI gailuak RM Image 4 Security Patches bertsiora eguneratu beharko lirateke, 01/2017 bertsiotik 05/2018 bertsiora (18-33400C).
- RM Shell 5 exekutatzen ari diren Pepperl Fuchs HMI gailuak RM Image 5 Security: Windows Cumulative Security Patch 07/2018 bertsiora eguneratu beharko lirateke (18-33624).
- Windows 7 edo Windows 10 exekutatzen duten Pepperl Fuchs HMI gailuak Windows Update eguneratze mekanismoaren bidez eguneratu beharko lirateke.
- Partxea zabalduta, konektatutako hirugarrenen bezero edo zerbitzari guztiek CredSSP protokoloaren azken bertsioa erabili behar dute.

Xehetasuna:

Erasotzaile batek kode arbitrarioa exekutatu lezake eta datu sentikorrak ikusi, bezero baten eta urrutiko zerbitzari baten arteko hasierako RDP konexioa antzemanez. MitM eraso bat behar da saioa kontrolatzeko. Ahultasun horretarako, CVE-2018-0886 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Ahultasuna

Hainbat ahultasun Schweitzer Engineering Laboratories Inc.-en Compass eta AcSELerator Architect produktuetan

Argitalpen data: 2018/07/11

Garrantzia: Handia

Kaltetutako baliabideak:

- Compass, 3.0.5.1 bertsioa eta aurrekoak
- AcSELerator Architect, 2.2.24.0 bertsioa eta aurrekoak (ICD package 2.38.0 bertsioa)

Azalpena:

Applied Risk-eko Gjoko Krstic ikertzaileak hainbat eratako ahultasunak identifikatu ditu Schweitzer Engineering Laboratories-en (SEL) Compass eta AcSELerator Architect produktuetan: baimen desegokiak, murrizpen desegokia entitateekiko erreferentzietan eta baliabideen kontrolik gabeko kontsumoa. Ahultasun horiek pribilegioen eskalatzea edo zerbitzuaren ukapena eragin lezakete.

Konponbidea:

- SEL Compass v3.0.6.1 edo ondorengoen kasuan, ondoko loturan eskuragarri dagoen eguneraketa ezarri: https://selinc.com/products/compass/#tab-downloads
- SEL AcSELerator v2.2.29.0 (ICD 2.44.0) edo ondorengoen kasuan, ondoko loturan eskuragarri dagoen eguneraketa ezarri: https://selinc.com/products/5032/#tab-downloads

Xehetasuna:

- Lehenetsitako baimen okerrak baliatuz erasotzaile batek sarbide osoa izan lezake Compassen direktorioetara, eta Compassen instalazio direktorioko fitxategiak alda edo gainidatz litzake. Horrela pribilegioen eskalatzea lor lezake eta kode gaiztoa exekutatu. Ahultasun horretarako CVE-2018-10604 identifikatzailea erreserbatu da.
- Kanpoko XML entitateei (XXE) egindako erreferentzietarako murrizpen desegokien ondorioz, erasotzaile batek AcSELerator Architecten XML parser-ari emandako sarrera ez egiaztatuak balia litzake datu arbitrarioak zabaltzea lortzeko, kode arbitrarioa exekutatzeko edo ukapen egoerak sortzeko. Ahultasun horretarako CVE-2018-10600 identifikatzailea erreserbatu da.
- Baliabideen kontrolik gabeko kontsumoa baliatuz, erasotzaile batek AcSELerator Architect-en FTP bezeroa erabil lezake zerbitzari gaizto batera konektatzeko. Horrek CPUaren erabileraren %100eko kontsumoa eragin lezake eta zerbitzuaren ukapen egoera eragin. Zerbitzua berrezartzeko beharrezkoa da aplikazioa berrabiatzea. Ahultasun horretarako CVE-2018-10608 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Universal Robots-en Robot Controllers-en

Argitalpen data: 2018/07/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- CB 3.1, SW 3.4.5-100 bertsioa.

Azalpena:

Politecnico di Milanoko hainbat ikertzailek, Trend Microko Forward-Looking Threat Research Team-ekin lankidetzan, pasahitz barneratu eta autentifikazio falta erako hainbat ahultasunen berri eman dute Universal Robotsen Robot Controllers produktuan. Urruneko erasotzaile batek gailuan kode arbitrarioa exekutatzea lor lezake.

Ohartarazi beharra dago Cesar Cerrudo eta Lucas Apak Hacking Robots Before Skynet-en aurkezpenean ahultasun honen berri eman zutela CVE-2018-10635 identifikatzailearekin.

Konponbidea:

Universal Robotsek ondoko ekintza prebentiboak aholkatzen ditu:

- Robotaren kontrol kaxarako eta programazio terminalerako sarbide fisikoa soilik konfiantzako erabiltzaileei baimentzea.
- Robota sare batera ez konektatzea, aplikazioak eskatzen ez duen bitartean behintzat.
- Robota ez konektatzea zuzenean Internetera. Sare seguru bat erabiltzea, suebakiaren konfigurazio zuzen batekin (TCP 30001 eta 30003 atakak murriztuta egon behar dira).
- Azpisare pribatu bat sortzea, robotaren sare interfazeak ahalik eta agerpen txikiena izan dezan.

Xehetasuna:

- Pasahitz barneratuen erabilpena. Aplikazioak kredentzial barneratuak erabiltzen ditu, eta horiek baliatuz erasotzaile batek kontrolatzailearen pasahitzak berrezar litzake. Ahultasun horretarako CVE-2018-10633 identifikatzailea erabili da.
- Autentifikazio falta funtzio kritikoan. TCP 30001 eta 30003 atakek URScript kode arbitrarioa entzuten dute, eta exekutatu egiten dute. Hori baliatuz ataketara sarbidea duen urruneko erasotzaile batek kodea exekuta lezake. Ahultasun horretarako CVE-2018-10635 identifikatzailea erabili da.

Etiketak: Ahultasuna

Hainbat ahultasun WAGOren e!DISPLAY-n

Argitalpen data: 2018/07/11

Garrantzia: Handia

Kaltetutako baliabideak:

- WAGO e!DISPLAY 762-3000
- WAGO e!DISPLAY 762-3001
- WAGO e!DISPLAY 762-3002
- WAGO e!DISPLAY 762-3003

Azalpena:

SEC-Consulteko T. Weber ikertzaileak hainbat eratako ahultasunak aurkitu ditu: XSS, sarrera parametroen egiaztapen okerra eta baimenen kudeaketa okerra. Erasotzaile batek ahultasun horiek balia litzake erabiltzailearen testuinguruan kode arbitrarioa exekutatzeko, dauden fitxategiak ordezkatzeko edo kode etengabea injektatzeko.

Konponbidea:

WAGOk firmwarearen azken bertsiora eguneratzea gomendatzen du (FW02). Eguneratzea ez bada posible, fabrikatzaileak sarbidea erabiltzaile eta gailu fidagarrietara murriztea gomendatzen du.
Firmware berria eskuratzeko moduari buruzko xehetasun gehiagotarako, fabrikatzailearen laguntza ekipokoarekin harremanetan jarri beharko duzu.

Xehetasuna:

- Web orria sortzen den bitartean sarreren neutralizazio oker batek (XSS) eragindako ahultasun bat baliatuz erasotzaile batek, autentifikazioarekin nahiz gabe, WBMan kodea injektatzeko bereziki diseinatutako eskaerak bidal litzake. Kode gaizto hori azken erabiltzailearen nabigatzailean renderizatu edo exekutatuko litzateke. Ahultasun horretarako CVE-2018-12981 identifikatzailea erreserbatu da.
- Fitxategi arriskutsuen kargan murrizpen desegoki batek eragindako ahultasun bat baliatuz, erasotzaile autentifikatu batek fitxategi arbitrarioak igo litzake fitxategien sistemara, web zerbitzariko baimenekin. Ahultasun horretarako CVE-2018-12980 identifikatzailea erreserbatu da.
- Baliabide kritikoetarako baimenen esleipen oker batek eragindako ahultasun bat baliatuz, erasotzaile batek sistemaren fitxategi kritikoak gainidatz litzake. Ahultasun horretarako CVE-2018-12979 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna

Zerbitzuaren ukapena Siemensen Ethernet EN100 komunikazio moduluetan eta SIPROTEC 5 erreleetan

Argitalpen data: 2018/07/12

Garrantzia: Handia

Kaltetutako baliabideak:

- EN100 Ethernet Module-rako IEC 61850 firmwarearen aldaerak, V4.33 baino lehenagoko bertsio guztiak
- EN100 Ethernet Module-rako PROFINET IO, Modbus TCP, DNP3 TCP eta IEC104 firmwarearen aldaerak, bertsio guztiak.
- CPUaren CP300 eta CP100 aldaerak eta dagozkien Ethernet komunikazio moduluak dituzten SIPROTEC 5 erreleak, V7.80 baino lehenagoko bertsio guztiak (soilik CVE-2018-11451 ahultasunak eragindakoak).
- CPUaren CP200 aldaerak eta dagozkien Ethernet komunikazio moduluak dituzten SIPROTEC 5 erreleak, bertsio guztiak (soilik CVE-2018-11451 ahultasunak eragindakoak).

Azalpena:

ScadaX-eko Victor Nikitin, Vladislav Suchkov eta Ilya Karpovek zerbitzuaren ukapen erako hainbat ahultasun aurkitu dituzte, Siemensen Ethernet EN100 komunikazio moduluei eta SIPROTEC 5 erreleei eragiten dietenak. Erasotzaile batek ahultasun horiek balia litzake kaltetutako produktuetan zerbitzuaren ukapena eragiteko.

Konponbidea:

- EN100ren IEC 61850 firmware aldaera: V4.33 bertsiora eguneratzea, hemen eskuragarri: https://support.industry.siemens.com/cs/us/en/view/109745821
- EN100ren PROFINET IO, Modbus TCP, DNP3 TCP eta IEC104 firmware aldaerak eta SIPROTEC 5, CPUaren CP200 aldaerarekin eta dagozkion Ethernet komunikazio moduluekin: TCP 102 atakarako sarbidea blokeatzea, kanpoko suebaki batekin esate baterako.
- SIPROTEC 5, CPUaren CP300 eta CP100 aldaerekin eta dagozkien Ethernet komunikazio moduluekin: Firmwarearen V7.80 bertsiora eguneratzea, ondoko gailu moten kasuan: 6MD85, 6MD86, 7SS85, 7KE85,7UM85, 7SA87, 7SD87, 7SL87, 7VK87, 7SA82, 7SA86, 7SD82, 7SD86, 7SL82, 7SL86, 7SJ86, 7SK82, 7SK85, 7SJ82, 7SJ85, 7UT82, 7UT85, 7UT86, eta 7UT87.

Xehetasuna:

- Sareko sarbidea lukeen erasotzaile batek bereziki diseinatutako pakete bat bidal lezake TCP 102 atakara, eta horrela kaltetutako produktuetan zerbitzuaren ukapen egoera sortu. SIPROTEC 4n EN100 moduluaren eta SIPROTEC Compact erreleen funtzionaltasuna berrezartzeko beharrezkoa da eskuz berrabiatzea. Aurrebaldintza modura, IEC 61850-MMS komunikazioa aktibatu beharra dago kaltetutako produktu edo moduluetan. Ahultasun horretarako CVE-2018-11451 identifikatzailea erabili da.
- Sareko sarbidea lukeen erasotzaile batek bereziki diseinatutako pakete bat bidal lezake TCP 102 atakara eta horrela zerbitzuaren ukapen egoera sor lezake EN100 komunikazio moduluan, oszilografoak exekutatzen ari baldin badira. EN100 moduluaren funtzionaltasuna berrezartzeko beharrezkoa da eskuz berrabiatzea. Aurrebaldintza modura, IEC 61850-MMS komunikazioa aktibatu beharra dago kaltetutako EN100 moduluetan. Ahultasun honek ez die eragiten SIPROTEC 5 erreleei. Ahultasun horretarako CVE-2018-11452 identifikatzailea erabili da.

Etiketak: Siemens, Ahultasuna

Bufferraren gainezkatzea Eaton-en 9000X Drive-n

Argitalpen data: 2018/07/13

Garrantzia: Ertaina

Kaltetutako baliabideak:

- 9000X Drive, 2.0.29 bertsioa eta lehenagokoak

Azalpena:

Ghirmay Desta ikertzaileak, Trend Microko Zero Day Initiativerekin lankidetzan, bufferraren gainezkatze erako ahultasun bat aurkitu du Eatonen 9000X Driven. Erasotzaile batek urrunetik kodea exekutatzea lor lezake kaltetutako gailuetan.

Konponbidea:

Eatonek v2.0.28 bertsioa argitaratu du 9000X Driverako, ahultasun hau konponduz. Ondoko loturatik deskargatu daiteke: http://www.eaton.com/Eaton/ProductsServices/Electrical/ProductsandServices/AutomationandControl/AdjustableFrequencyDrives/IndustrialDrives/SVX/index.htm#tabs-4

Xehetasuna:

Kaltetutako produktuek daukaten bufferraren gainezkatze erako ahultasun bat baliatuz, erasotzaile batek kodea exekuta lezake urrunetik. Ahultasun horretarako CVE-2018-8847 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Baliabideen kontsumo ez-kontrolatua Moxa-ren Nport 5210, 5230 eta 5232n

Argitalpen data: 2018/07/20

Garrantzia: Handia

Kaltetutako baliabideak:

Nport 5210, 5230 eta 5232, 2.9 build 17030709 bertsioa eta lehenagokoak.

Azalpena:

Mikael Vingaardek ahultasun honen berri eman dio NCCIC/ICS-CERTi. Erasotzaile batek ahultasun hau balia lezake TCP SYN paketeak bidaliz baliabide guztiak kontsumitzearren, eta gailua ez eskuragarri moduan utziz.

Konponbidea:

Moxa-k erabiltzaileei aholkatzen die firmwarearen azken bertsiora eguneratzea, hemen eskuragarri:

https://www.moxa.com/support/download.aspx?type=support&id=904

Xehetasuna:

Erasotzaile batek eska lezakeen baliabideen kopurua ez dago mugatuta, eta beraz, ahultasun hori balia liteke eskuragarri dauden baliabideak kontsumitzeko, zerbitzuaren ukapena eraginez. Ahultasun horretarako CVE-2018-10632 identifikatzailea erabili da.

Etiketak: Ahultasuna

Hainbat ahultasun Echelon-en SmartServer 1, SmartServer 2,

i.LON 100 eta i.LON 600en

Argitalpen data: 2018/07/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SmartServer 1, i.LON 100 eta i.LON 600, bertsio guztiak
- SmartServer 2, 4.11.007 bertsioa baino lehenagoko guztiak

Azalpena:

Echelonek, Daniel Crowley eta IBMren X-Force Red Teamekin batera, ahultasun hauen berri eman dio NCCIC/ICS-CERTi. Ahultasun horiek arrakastaz baliatuz gero, gailuan urrunetik kodea exekutatu liteke.

Konponbidea:

Echelonek kaltetutako erabiltzaileei gomendatzen die SmartServer 2 Service Pack 7 (4.11.007 bertsioa) instalatzea CVE-2018-8859, CVE-208-8851 eta CVE-2018-8855en kalteak arintzeko. Ondoko loturatik deskarga daiteke:

https://www.echelon.com/software-downloads?ele=153-0608-01A

Ondoren azaltzen den eskuzko arintzea egitea ere gomendatzen du:

CVE-2018-10627rako Echelonek kaltetutako erabiltzaileei aholkatzen die WebParams.dat fitxategia aldatzea.

SmartServer 2 Service Pack 7 instalatu bitartean, Echelonek ondoren azaltzen den arintzea ezartzea aholkatzen du:

- SmartServer eta i.LON 600 gailu guztiak, SmartServer eta i.Lon zerbitzuak erabiltzen dituzten zerbitzariekin batera, suebaki baten atzean instalatu behar dira edo beste gailurik gabeko VLAN batean.
- Hasierako instalazioan aldatu kaltetutako produktuen erabiltzaile izena eta pasahitza.
- SmartServer edo i.LON 100en kasuan desgaitu zerbitzu ez zifratuak eta zerbitzu zifratu seguruak.

Xehetasuna:

- **Informazioaren agerpena:** Erasotzaile batek API SOAP erabil lezake konfigurazio sentikorreko elementuak berreskuratzeko eta aldatzeko, esate baterako, web eta FTP zerbitzarien erabiltzaile izenak eta pasahitzak. Ahultasun horrek ez dio eragiten i.LON 600 produktuari. Ahultasun horretarako CVE-2018-10627 identifikatzailea erabili da.
- **Autentifikazioa saihestea ordezko bide edo kanal bat erabiliz:** Erasotzaile batek segurtasuneko konfigurazioaren fitxategian zehaztuta dagoen derrigorrezko autentifikazioa saihets lezake, direktorioaren izenean karaktere gehigarriak idatziz sartu nahi den direktorioa zehazteko unean. Ahultasun horrek ez dio eragiten i.LON 600 produktuari. Ahultasun horretarako CVE-2018-8859 identifikatzailea erabili da.
- **Kredentzialen biltegiratzea babesik gabe:** Gailuek pasahitzak testu gardenean gordetzen dituzte, eta ahultasun hori baliatuz konfigurazio fitxategira sarbidea lukeen erasotzaile batek SmartServer-en web erabiltzailearen interfazean saioa has lezake. Ahultasun horretarako CVE-2018-8851 identifikatzailea erabili da.
- **Informazio sentikorraren transmisioa testu gardenean:** Gailuek web konexioak zifratu lehenetsirik gabe baimentzen dituzte eta konfigurazio eta firmware eguneraketak jaso ditzakete FTP ez-seguruen bidez. Ahultasun horretarako CVE-2018-8855 identifikatzailea erabili da.

Etiketak: Ahultasuna

Hainbat ahultasun AVEVAren InduSoft eta InTouch softwarean

Argitalpen data: 2018/07/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- InduSoft Web Studio v8.1 eta v8.1 SP1.
- InTouch Machine Edition v2017 8.1 eta v2017 8.1 SP1.
- InTouch 2014 R2 SP1 eta lehenagokoak.
- InTouch 2017.
- InTouch 2017 Update 1.
- InTouch 2017 Update 2.

Azalpena:

CyberXeko George Lashenkok eta Tenable Researcheko ikertzaileek bufferraren gainezkatze erako ahultasunak aurkitu dituzte. AVEVAren InduSoft eta InTouch softwarearekin zerikusia dute, eta horiek baliatuz urruneko erasotzaile batek kodea exekuta lezake.

Konponbidea:

InduSoft Web Studio v8.1 SP1eko erabiltzaileek lehenbailehen instalatu behar dute InduSoft Web Studio Hotfix 81.1.00.08 partxea. InduSoft Web Studio v8.1eko erabiltzaileek SP1 bertsiora eguneratu behar dute, eta ondoren partxea instalatu.

InTouch Machine Edition 2017 v8.1 SP1eko erabiltzaileek lehenbailehen instalatu behar dute InTouch Machine Edition Hotfix 81.1.00.08 partxea. InTouch Machine Edition 2017 v8.1eko erabiltzaileek SP1 bertsiora eguneratu behar dute, eta ondoren aplikatu partxea.

http://www.indusoft.com/File-Management?Command=Core_Download&EntryId=2074

https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=5063

InTouch 2014 R2 SP1 softwarearen kasuan, HF-11_1_SP1/CR149705 partxea lehenbailehen ezarri behar da. Bertsio zaharragoetako erabiltzaileek lehenbizi partxedun bertsio batera eguneratu behar dute, eta ondoren partxea instalatu.

https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=5057

InTouch 2017 Update 2rako partxea HF-17_2/CR149706 da. Bertsio zaharragoek lehenbizi Update 2ra eguneratu behar dute, eta ondoren partxea instalatu.

https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=5058

Xehetasun gehiago erreferentziazko loturetan aurki daitezke.

Xehetasuna:

- **Bufferraren gainezkatzea InduSoft Web Studio eta InTouch Machine Edition-en**: Bufferraren gainezkatzearen ahultasun hori baliatzeko, urruneko erasotzaile batek bereziki diseinatutako eskaerak bidal litzake, zenbait etiketa, alarma edo gertaeratan irakurketa edo idazketa eskaeren ekintza batzuk gertatzen diren bitartean. Horren bitartez urrunetik kodea exekuta liteke. Ahultasun horretarako CVE-2018-10620 identifikatzailea erabili da.
- **Bufferraren gainezkatzea InTouch-en:** Koma mugikorrean osokoek duten kudeaketa oker baten ondorioz, sisteman autentifikaziorik ez duen erasotzaile batek bereziki diseinatutako pakete bat bidal lezake bufferraren gainezkatzea eragiteko. Ahultasun hori baliatuz kodea exekuta liteke InTouch View-ren prozesuak dituen pribilegio berdinekin. Ahultasun horretarako CVE-2018-10628 identifikatzailea erabili da.

Etiketak: 0day, Ahultasuna

Hainbat ahultasun MicroSCADA Pro SYS600-n

Argitalpen data: 2018/07/23

Garrantzia: Kritikoa

Kaltetutako baliabideak:

MicroSCADA Pro SYS600 9.2, 9.3, 9.4

Azalpena: Kaspersky Labseko Vladimir Dashchenko ikertzaileak ahultasun honen berri eman du goian aipatutako produktuaren bertsioetan. Autentifikatutako erasotzaile batek ahultasun hau balia lezake, eta ondorioz, prozesuaren urruneko blokeoa eragin liteke edo kaltetutako sisteman kode arbitrarioa exekutatu.

Gainera, Microsoftek arazo ezagun bat dokumentatu du (berrabiarazpen buklea), Sentinel HASP kontrolatzaile zaharrekin, Microsoften segurtasun eguneraketak ezartzerakoan 2018ko martxoan eta hurrengoetan. ABBk konfirmatu ditu buklearen berrabiarazpen arazoak Windows 7 eta Windows Server 2008 SP2 sistemekin gutxienez. Ohar honen argibideak jarraitzea gomendatzen da Sentinel HASP / LDK 7.80 bertsioa kontrolatzaile berrienekin instalatzeko, Microsoften segurtasun eguneraketak ezarri aurretik.

Konponbidea:

Arazoa Gemaltok konpondu du produktuaren hurrengo bertsioan:

- Sentinel HASP/LDK License Manager-en 7.80 bertsioa

ABBk kaltetutako erabiltzaileei gomendatzen die eguneraketa hori lehenbailehen instalatzea.

Eguneraketa ondoko sistema eragileetan erabil daiteke: Windows 7 SP1, Windows 8.1 SP1, Windows Server 2008 R2 SP1, Windows Server 2012 R2, Windows Server 2016, Windows 10 Version 1709. Sistema eragilearen bertsio zaharragoak ere seguruenik erabat bateragarriak izango dira, baina Gemaltok ez du horrelakorik bermatzen. Goian aipatutako sistema eragileez gain, ABBk eguneraketa Windows Server 2008 SP2-n probatu du.

Xehetasuna:

Urrunetik kode arbitrarioa exekutatzea: Sentinel HASP Run-time Environment zerbitzuan dagoen ahultasun bat balia lezake erasotzaile batek urrunetik, bereziki sortutako fitxategi bat bertara igoz eta bufferraren gainezkatzea eraginez. Horrela kode arbitrarioa exekuta liteke edo urrunetik prozesua itzali (zerbitzuaren ukapena). Ahultasun horietarako honako identifikatzaileak erabili dira: CVE-2017-11498, CVE-2017-11497, CVE-2017-11496, CVE-2017-12818, CVE-2017-12819, CVE-2017-12820, CVE-2017-12821, CVE-2017-12822.

Etiketak: SCADA, Ahultasuna

Bufferraren hainbat gainezkatze Wecon-en LeviStudioU-n

Argitalpen data: 2018/07/27

Garrantzia: Kritikoa

Kaltetutako baliabideak:

LeviStudioU

Azalpena:

Nfocuseko segurtasun ekipoak eta Trend Microko Zero Day Initiativeko Mat Powell ikertzaileak bufferraren gainezkatze erako hainbat ahultasunen berri eman dute, Wecon fabrikatzailearen LeviStudioU softwareari eragiten diotenak. Ahultasun horiek baliatuz erasotzaile batek urrunetik kodea exekuta lezake administratzaile baimenekin.

Konponbidea:

Une honetan ez dago inolako arintze edo konponbiderik ahultasun horietarako.

Kaltetutako softwarea erabiltzen duten gailuak isolatzea eta horietarako sarbideak kontrolatzea gomendatzen da.

Gainera, kaltetutako baliabideak babesteko ondokoa gomendatzen da:

- 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:

Fitxategi batzuek, UMP, HSC edo HGCM bezalakoak, dauzkaten hainbat eremutan ez dute luzeraren tratamendu zuzena egiten. Egoera horrek bufferraren gainezkatzea eragiten du. Beste fitxategi zehatzago batzuk, UserMgr.xml, TTS.xml edo UserManage.exe bezalakoek eta abarrek ere, arazoak dauzkate bai parametroak eta bai dauzkaten beste elementu batzuk kudeatzerakoan.

Zero Day Initiativek ZDI-18-784tik ZDI-18-873ra bitarteko identifikatzaileak erabili ditu ahultasun kritiko hauetarako.

Etiketak: 0day, Ahultasuna

Hainbat ahultasun Hirschmann produktuen TCPdump funtzionaltasunetan

Argitalpen data: 2018/07/30

Garrantzia: Handia

Kaltetutako baliabideak:

- HiOS, 07.0.00 bertsioa eta lehenagokoak ondorengo produktuetan:
  - RSP
  - RSPE
  - RSPS
  - RSPL
  - MSP
  - EES
  - EESX
  - GRS
  - OS
  - RED
- Classic, ondoko produktuen bertsio guztiak:
  - RS
  - RSR
  - RSB
  - MACH100
  - MACH1000
  - MACH4000
  - MS
  - OCTOPUS
- Cellular Router, 01.2.02 bertsioa eta lehenagokoak ondoko produktuan:
  - OWL

Azalpena:

Beldenek TCPdump funtzionaltasunen hainbat ahultasunen berri eman du Hirschmannen produktuen familia eta plataforma ezberdinetan. Bufferraren gainezkatzearen ahultasun hauek baliatuz urruneko erasotzaile batek zerbitzuaren ukapenak eragin litzake edo urrunetik kodea exekutatu.

Konponbidea:

Fabrikatzaileak bere bezeroei gomendatzen die produktuak lehenbailehen eguneratzea, posible den heinean behintzat.

- HiOS: Produktu guztiak 07.0.01 bertsiora eguneratzea.
- Classic: Produktu hauetarako ez da aurreikusten inolako eguneraketarik.
- Cellular Router:
  - OWL LTE M12: 01.2.03 bertsiora eguneratzea.
  - OWL LTE, OWL 3G: Konponbidea 02.0.00 bertsiorako dago aurreikusita.

Xehetasuna:

TCPdumpen barnean (4.9.2 bertsioa baino lehenagokoak) sartuta dauden funtzioak egiten dituzten sarrera parametroen tratamendu okerra baliatuz, urruneko erasotzaile batek zerbitzuaren ukapenak eragin litzake edo kodea exekutatu.

Ahultasunak soilik balia daitezke saio aktibo batek bere jardunean zehar TCPdump funtzioak erabiltzen baditu eta sareko trafikoa kaltetutako gailuak zuzenean kudeatzen badu. TCPdump funtzionaltasuna berez inaktibo dago.

Ahultasun horietarako honako identifikatzaileak erabili dira: CVE-2017-12894, CVE-2017-12996, CVE-2017-12988, CVE-2017-13012, CVE-2017-13013, CVE-2017-13022, CVE-2017-13030, CVE-2017-13037, CVE-2016-7923, CVE-2016-7926, CVE-2016-7932, CVE-2016-7936, CVE-2016-7974, CVE-2016-7975, CVE-2016-7983, CVE-2016-7984.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna