2020ko Urriaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Bosch produktuen ahultasunak

Argitalpen data: 2020/10/01

Garrantzia: Altua

Kaltetutako baliabideak:

- Bosch PRAESENSA, 1.10 bertsioa eta aurrekoak;
- Bosch PRAESENSA, 4.41 bertsioa eta aurrekoak.

Azalpena:

Bosch etxeak PRAESIDEO Network Controller eta PRAESENSA System Controller produktuetan antzemandako 3 ahultasunen berri eman du; 2 larritasun kritikokoak dira, eta beste bat tartekoa. Horien bidez, erasotzaile batek ekintza arbitrarioak burutu litzake edo Cross-Site-Scripting (XSS) biltegiratuaren motako erasoak burutu.

Konponbidea:

- PRAESIDEO 4.42 eta PRAESENSA 1.20 bertsioetara eguneratzea.
- LBB4401/00 eta PRS-NCO-B Network Controllers kontrolatzaileak ezin dira PRAESIDEO 4.42 bertsiora eguneratu, beraz, sarea sare publikotik isolatzea gomendatzen da. Hori posible ez balitz, firewall erabiltzea gomendatuko litzateke.

Xehetasunak:

- Bosch PRAESIDEO eta Bosch PRAESENSA produktuen webgunean oinarritutako interfazeko ahultasuna baliatuta, baimenik gabeko urrutiko erasotzaile batek ekintza arbitrarioak burutu litzake sistema batean, beste erabiltzaile baten izenean (Cross-Site Request Forgery). Horrek esan nahi du biktima engainatua izango dela lotura maltzur batean klik egiteko, edo formulario maltzur bat bidaltzeko. Larritasun handiko ahultasun horretarako CVE-2020-6776 identifikatzailea esleitu da.
- Bosch PRAESIDEO produktuetan erabilitako GoAhead web zerbitzariak ez du behar den moduan babesten HTTP Digest baimen-saiakeretan. Larritasun handiko ahultasun horretarako CVE-2020-15688 identifikatzailea esleitu da.
- Bosch PRAESIDEO eta Bosch PRAESENSA produktuen webgunean oinarritutako kudeaketa interfazeko ahultasun baten bidez, urrutiko erasotzaile batek, baimenarekin, administrari pribilegioekin, Cross-Site-Scripting (XSS) eraso bat burutu lezake, beste erabiltzaile baten aurka. Biktima kudeaketa interfazera konektatzean, biltegiratutako kodea nabigatzailearen testuinguruan exekutatzen da. Tarteko larritasuna duen ahultasun horretarako CVE-2020-6777 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun WAGO produktu batzuetan

Argitalpen data: 2020/10/01

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Produktu hauen firmware 07 bertsioak eta aurrekoak:

- 750-852;
- 750-880/xxx-xxx;
- 750-881;

- 750-831/xxx-xxx;
- 750-882;
- 750-885/xxx-xxx;
- 750-889.

Produktu hauen firmware 03 bertsioak eta aurrekoak:

- 750-362;
- 750-363;
- 750-823;
- 750-832/xxx-xxx;
- 750-862;
- 750-891;
- 750-890/xxx-xxx.

Produktu hauen firmware 13 bertsioak eta aurrekoak:

- 750-352;
- 750-831/xxx-xxx;
- 750-852;
- 750-880/xxx-xxx;
- 750-881;
- 750-889.

Azalpena:

Maxim Rupp eta Secuninja ikertzaileek, biak erakundeak koordinatuta, WAGO produktuetan antzemandako larritasun kritiko, handi eta ertaineko 3 ahultasunen berri eman dute. Fabrikatzaileari berari ere jakinarazi dizkiote.

Konponbidea:

Produktu hauen firmware 07 bertsioen ostekoetara eguneratzea:

- 750-852;
- 750-880/xxx-xxx;
- 750-881;
- 750-831/xxx-xxx;
- 750-882;
- 750-885/xxx-xxx;
- 750-889.

Produktu hauen firmware 03 bertsioen ostekoetara eguneratzea:

- 750-362;
- 750-363;
- 750-823;
- 750-832/xxx-xxx;
- 750-862;
- 750-891;
- 750-890/xxx-xxx.

Produktu hauen firmware 14 bertsiora edo ostekoetara eguneratzea:

- 750-352;
- 750-831/xxx-xxx;
- 750-852;
- 750-880/xxx-xxx;
- 750-881;
- 750-889.

Xehetasunak:

- Ahultasun hori baliatuta, WBM (Web-Based Management) sarbidea duen erasotzaile batek aplikazioaren karga saihestuko luke exekuzio-denboran, bereziki diseinatutako eskaerak bidaliz gailua berrabiarazita. Ahultasun horretarako, CVE-2020-12505 identifikatzailea esleitu da.
- Ahultasun horren bidez, WBMrako sarbidea eta direktorioen egiturari buruzko ezagutza duen erasotzaile batek, gailuen parametroen konfigurazioa aldatu lezake, bereziki diseinatutako eskaerak baimenik gabe bidaliz. Horrela, aplikazioa oker funtzionatzen has liteke, berrabiarazi ostean. Ahultasun horretarako, CVE-2020-12506 identifikatzailea esleitu da.
- Gailuaren SNMP konfigurazio-orria XSS eraso iraunkor baten mende egon liteke. Erasotzaile batek gailuan baimenarekin hasi beharko luke saioa SNMP konfigurazio webgunea script maltzurrekin urratzeko. Horren ondorioz, kode maltzur bat instalatu eta informazio konfidentziala lortzeko erabil liteke. Ahultasun horretarako, CVE-2018-16210 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, Ahultasuna.

Baimen-omisioa IBM Maximo Asset Management sisteman

Argitalpen data: 2020/10/02

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- IBM Maximo Asset Management, 7.6.0 eta 7.6.1 bertsioak.
- Industria konponbideen arloko produktu kaltetuak, core bertsio kaltetu bat erabiliz gero:
-
    - Abiaziorako Maximo;
    - Zientzietarako Maximo;
    - Energia nuklearrerako Maximo;
    - Petrolio eta gaserako Maximo;
    - Garraiorako Maximo;
    - Erabileretarako Maximo.
- IBM Control Desk produktu kaltetuak, core bertsio kaltetu bat erabiliz gero:
    - SmartCloud Control Desk;
    - IBM Control Desk;
    - Tivoli Integration Composer.

Azalpena:

IBM erakundeak larritasun kritikoko ahultasun bat argitaratu du. Horren bidez, erasotzaile batek baimen-omisioa eragin lezake.

Konponbidea:

Kaltetutako produktuari dagokion Interim Fix edo Fix Pack aplikatzea.

- 7.6.1.2 bertsiorako:
    - Maximo Asset Management 7.6.1.2 Feature Pack aplikatzea, 7.6.1.2-TIV-MAMMT-FP002 edo eskuragarri dagoen azken Interim Fix.
- 7.6.1.0 bertsiorako:
    - Maximo Asset Management 7.6.1.1 iFix aplikatzea, 7.6.1.1-TIV-MBS-IFIX002 edo eskuragarri dagoen azken Interim Fix.
- 7.6.1.0 bertsiorako:
    - Maximo Asset Management 7.6.1.0 iFix aplikatzea, 7.6.1.0-TIV-MBS-IFIX012 edo eskuragarri dagoen azken Interim Fix.
- 7.6.1.10 bertsiorako:
    - Maximo Asset Management 7.6.0.10 iFix aplikatzea, 7.6.0.10-TIV-MBS-IFIX003 edo eskuragarri dagoen azken Interim Fix.

Xehetasunak:

Bereziki diseinatutako HTTP komando baten bidez, erasotzaile bat baimenik gabe sar liteke, eta komandoak exekutatu. Ahultasun horretarako, CVE-2020-4493 identifikatzailea esleitu da.

Etiketak: Eguneratzea, IBM, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun PEPPERL FUCHS Comtrol RocketLinux sisteman

Argitalpen data: 2020/10/08

Garrantzia: Kritikoa

Kaltetutako baliabideak:

P F Comtrol RocketLinx, bertsioak:

- ES7510-XT,
- ES8509-XT,
- ES8510-XT,
- ES9528-XTv2,
- ES7506,
- ES7510,
- ES7528,
- ES8508,
- ES8508F,
- ES8510,
- ES8510-XTE,
- ES9528/ES9528-XT.

Azalpena:

EC Consult Vulnerability Lab enpresako T. Weber ikertzaileak, erakundeak koordinatuta, hainbat ahultasun antzeman ditu PEPPERL FUCHS Comtrol RocketLinux sisteman, eta fabrikatzaileari horien berri eman dio.

Konpobidea:

Gaur egun, fabrikatzaileak ez du ahultasun horiek konpontzeko eguneratzerik argitaratu, beraz, kanpo babes neurriak eskatu dira:

- Firewall baten bidez gailurako konfiantzazkoak ez diren sareen trafikoa blokeatu behar da, bereziki administrazio webgunera zuzendutako trafikoari dagokionez.
- Administrari eta erabiltzaile sarbidea pasahitz seguru baten bidez babestua egon behar da, eta pertsona talde oso mugatu batentzako soilik egon behar da eskuragarri.

Xehetasunak:

Urrutiko erasotzaileek hainbat ahultasun baliatu litzakete gailura sartzeko, edozein programa exekutatu eta informazioa lortzeko.

- Baimen desegokiko ahultasun horretarako CVE-2020-12500 identifikatzailea esleitu da.
- CVE-2020-12501 identifikatzailea esleitu da softwareko kredentzial barneratuen motako ahultasun kritiko horretarako.
- CVE-2020-12502 identifikatzailea esleitu da CSRF (Cross-Site Request Forgery) motako ahultasun horretarako.
- Sarbide-balioztatze desegokiko ahultasun horretarako CVE-2020-12503 identifikatzailea esleitu da.
- Funtzionalitate ezkutuko ahultasun kritiko horretarako CVE-2020-12504 identifikatzailea esleitu da.

Etiketak: Komunikazioak, IoT, Ahultasuna

Johnson Controls enpresaren American Dynamics victor Web Client eremuan baimen desegokia gertatu da

Argitalpen data: 2020/10/09

Garrantzia: Altua

Kaltetutako baliabideak:

American Dynamics victor Web Client, bertsio guztiak 5.4.1era arte, hori barne.

Azalpena:

Joachim Kerschbaumer-ek Johnson Controls enpresari larritasun handiko ahultasun baten berri eman dio, baimen desegokiaren motakoa.

Konponbidea:

Produktua eguneratzea 5.6 bertsiora.

Xehetasunak:

American Dynamics victor Web Client izeneko sistemak ez du baimena egiaztatzen, eta, ondorioz, ondoko sare batetik sartu den erasotzaile bat sistemako artxibo arbitrarioak ezabatzen saiatu da. Ahultasun horretarako, CVE-2020-9048 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, Ahultasuna.

Bilaketa ibilbidearen ahultasun ez fidagarria Flexera InstallShield sisteman

Argitalpen data: 2020/10/14

Garrantzia: Altua

Kaltetutako baliabideak:

- Flexera InstallShield, 2015 SP1 bertsiora artekoak;
- Flexera InstallShield sistema beste enpresa batzuek saldutako produktu askotan integratuta dago.

Azalpena:

Ikertzaile anonimo batek fabrikatzaileari eman dio larritasun handiko ahultasun baten berri, bilaketa-ibilbide ez fidagarriaren motakoa.

Konponbidea:

Erabiltzaileei gomendatu zaie produktuaren hornitzailearen laguntza-taldearekin harremanetan jartzeko, ahultasun hau konpontzeko aukeren berri izateko. Informazio gehiago izateko, kontsultatu Flexeraren KBR artikulua.

Xehetasunak:

Kaltetutako produktua bilaketa-ibilbide ez fidagarriaren motako ahultasun baten mende dago. horren bidez, erasotzaile batek DLL maltzur bat exekuta lezake, instalazio programaren artxibo exekutagarriaren lan-direktorioan kokatuko balitz, ingeniaritza sozialaren metodoen bidez. Ahultasun horretarako, CVE-2016-2542 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Microsoft, Ahultasuna, Windows.

Hainbat ahultasun MOXA NPort IAW5000A-I/O Series sisteman

Argitalpen data: 2020/10/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

NPort IAW5000A-I/O 2.1 firmware bertsioarekin edo aurreko batekin.

Azalpena:

Evgeniy Druzhinin eta Ilya Karpov de Rostelecom-Solar ikertzaileek sei ahultasun antzeman dituzte MOXA NPort IAW5000A-I/O Series sisteman. Horien bidez, urrutiko erasotzaile batek informazio konfidentziala eskuratu lezake, saioak bahitu edo sarbidea lortu, erabiltzaile batek administrari pribilegioak erabil ditzan utzi edota pasahitz ahulak erabili.

Konponbidea:

Moxak firmware bertsio bat argitaratu du ahultasun horiek konpontzeko.

Xehetasunak:

MOXA NPort IAW5000A-I/O Series sisteman aurkitutako larritasun kritikoena produktu honetan integratutako web zerbitzuari dagokio, eta pasahitz ahulak erabil litzake, ez die erabiltzaileei pasahitz segururik eskatzen. Ahultasun horretarako, CVE-2020-25153 identifikatzailea esleitu da.

MOXA NPort IAW5000A-I/O Series sisteman aurkitutako beste ahultasun batzuek honako identifikatzaileak dituzte: CVE-2020-25198, CVE-2020-25194, CVE-2020-25190, CVE-2020-25196 eta CVE-2020-25192.

Etiketak: Eguneratzea, Azpiegitura kritikoak, SCADA, Ahultasuna.

Schneider Electric erakundearen produktuen ahultasunak

Argitalpen data: 2020/10/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- M340 CPUs: BMX P34x, 3.20ren aurreko firmware bertsioak.
- M340 Communication Ethernet moduluak:
  - BMX NOE 0100 (H), 3.3ren aurreko bertsioak;
  - BMX NOE 0110 (H), 6.5ren aurreko bertsioak;
  - BMX NOC 0401, 2.10en aurreko bertsioak.
- Ethernet COPRO integratua duten premium prozesatzaileak: TSXP574634, TSXP575634 eta TSXP576634, 6.1en aurreko bertsioak.
- Premium komunikazio moduluak:
  - TSXETY4103, 6.2ren aurreko bertsioak;
  - TSXETY5103, 6.4ren aurreko bertsioak.
- Ethernet COPRO integratua duten quantum prozesatzaileak: 140CPU65xxxxx, 6.1en aurreko bertsioak.
- Quantum komunikazio moduluak:
  - 140NOE771x1, 7.1en aurreko bertsioak;
  - 140NOC78x00, 1.74ren aurreko bertsioak;
  - 140NOC77101, 1.08ren aurreko bertsioak.
- Produktu hauen bertsio guztiak:
  - EcoStruxure Machine Expert (SoMachine eta SoMachine Motion gisa ezagunak);
  - E PLC400;
  - E PLC100;
  - E PLC_Setup;
  - EcoStruxure Machine SCADA Expert.
- Acti9:
  - Smartlink SI D, 002.004.002 bertsioaren aurreko bertsio guztiak;
  - Smartlink SI B, 002.004.002 bertsioaren aurreko guztiak;
  - PowerTag Link / Link HD, 001.008.007 bertsioaren aurreko guztiak;
  - Smartlink EL B, 1.2.1 bertsioaren aurreko guztiak.
- Wiser:
  - Link, 1.5.0en aurreko bertsio guztiak;
  - Energy, 1.5.0ren aurreko bertsio guztiak.
- EcoStruxure™:
  - Power Monitoring Expert, 9.0, 8.x eta 7.x bertsioak;
  - Energy Expert, 2.0 bertsioa:
  - Power SCADA Operation Advanced Reporting Dashboards Module sistemekin, 9.0 bertsioa.
- Power Manager, 1.1, 1.2 eta 1.3 bertsioak.
- StruxureWareTM PowerSCADA Expert Advanced Reporting eta Dashboards Module sistemekin, 8.x bertsioak.

Azalpena:

Schneider Electric erakundeak hainbat ahultasunen berri eman du: 2 kritikoak, 7 handiak eta 2 tartekoak. Motak: kredentzialen kudeaketa, memoria korrupzioa, egiaztatu gabeko eremu-luzera, lizentzia artxibo arbitrarioak sortzea, urruneko komunikazioa CodeMeter API delakoarekin, lizentzia artxiboen aldaketa edo sorkuntza, heap informazioa duten paketeen itzulera, nahiko aleatorioak ez diren balioak, sarbide kontrol desegokia eta sarbidearen neutralizazio desegokia

webgune bat sortu bitartean.

Konponbidea:

Fabrikatzailearen abisu bakoitzeko Remediation atalean azaldutako eguneratze eta konfigurazio jarraibideei kasu egitea.

Xehetasunak:

Larritasun kritikoko ahultasunak ondoren azalduta daude:

- Kredentzialen kudeaketa arloko ahultasun bat dago. Web zerbitzarian baimenik gabeko komandoak exekuta litezke, bereziki diseinatutako HTTP eskaerak bidalita. Ahultasun horretarako, CVE-2020-7533 identifikatzailea esleitu da.
- Memoriaren korrupzioaren motako ahultasun bat dago. Horren bidez, CodeMeter paketeen analizatzailearen mekanismoak (7.10a bertsioaren aurreko guztiak) ez du eremuen luzera egiaztatzen. Erasotzaile batek paketeak bidal litzake, bereziki diseinatuak, ahultasun hori baliatzeko. Ahultasun horretarako, CVE-2020-14509 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak esleitu dira: CVE-2020-14513, CVE-2020-14515, CVE-2020-14517, CVE-2020-14519, CVE-2020-16233, CVE-2020-7548, CVE-2020-7545, CVE-2020-7546 eta CVE-2020-7547.

Etiketak: Eguneratzea, Azpiegitura kritikoak, SCADA, Schneider Electric, Ahultasuna.

Bufferrak gainezka egitea Fieldcomm Group HART-IP eta hipserver sistemetan

Argitalpen data: 2020/10/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- HART-IP Developer kit, 1.0.0.0 bertsioa;
- hipserver, 3.6.1 bertsioa.

Azalpena:

Dragos, Inc erakundeko Reid Wightman ikertzaileak bufferraren gainezkatze motako ahultasun bat deskubritu du. Horren bidez, erasotzaile batek gailua blokeatu lezake, edo kodearen urrutiko exekuzioa burutu.

Konponbidea:

Fieldcomm Group erakundeak erabiltzaileei gomendatu die software hori exekutatzen duten ekipoei sarbidea mugatzeko. Hipserver erabiltzaileen 3.7.0 bertsiora edo osteko batera eguneratu behar dute.

Xehetasunak:

Fieldcomm Group HART-IP eta hipserver sistemetan antzemandako ahultasuna HART-IP mezuen bidez erabil liteke karga erabilgarri nahiko handiekin, pilan oinarritutako buffer gainezkatzea eraginez. Horrela, gailua blokeatu liteke, edota gailuaren beraren kontrola lortu. Ahultasun horretarako, CVE-2020-16209 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Sarbide desegokia balioztatzea Aprecher Automation erakundearen SPRECON-E sisteman

Argitalpen data: 2020/10/15

Garrantzia: Altua

Kaltetutako baliabideak:

SPRECON-E, 8.64b bertsioaren aurreko firmware bertsioak.

Azalpena:

Gregor Bonney izeneko langileak, Innogy-ko CyberRange-e zentrokoa, larritasun handiko ahultasun baten berri emateko oharraren argitalpena koordinatu du. Mota: sisteman konfigurazio-artxiboaren sarbide desegokia SPRECON-E sisteman.

Konponbidea:

SPRECON-E 8.64b firmware bertsiora eguneratzea. Gainera, fabrikatzaileak firmwarearen bertsio eguneratua eskaintzen du, egun 8.64d, beren aholkularien bidezko bezeroentzat.

Xehetasunak:

8.64b bertsioaren aurreko Sprecher SPRECON-E firmwarearen bidez, tokiko erasotzaile batek kode arbitrarioa sartu lezake. Firmware horrek ez dauka sarrerako balioen balioztatzerik gailuaren aldean. Ingeniaritza softwareak eman ohi du, parametrizazioan. Beraz, tokiko konfigurazioko artxiboetarako sarbidea duen erasotzaile batek komando maltzurrak sartu litzake, konpilatu ostean parametro baliodunen ("PDL") artxiboetan exekutatzeko, gailura transferitu eta berrabiarazteko.

Ahultasun horretarako, CVE-2020-11496 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun Advantech produktu batzuetan

Argitalpen data: 2020/10/16

Garrantzia: Altua

Kaltetutako baliabideak:

- WebAccess/SCADA, 9.0 bertsioa eta aurrekoak;
- R-SeeNet, 1.5.1etik 2.4.10erako bertsioak.

Azalpena:

Trend Micro erakundeko ZDIko Sivathmican Sivakumaran ikertzaileek eta rgod izenez ezaguna denak, Trend Micro erakundeko ZDIrekin lankidetzan, 2 ahultasunen berri eman dute, biak larritasun handikoak, artxibo izen edo ibilbidearen kanpo kontrol edo SQL injekzio motakoak.

Konponbidea:

- WebAccess/SCADA 9.0.1. bertsiora edo ostekoetara eguneratzea;
- R-SeeNet 2.4.11 bertsiora edo ostekoetara eguneratzea.

Xehetasunak:

- WebAccess/SCADA sistemako WADashboard osagaiaren bidez, erasotzaile batek artxiboen sistemako operazio batean erabilitako ibilbide batean eragin lezake edo kontrolatu lezake, administrari gisa kodea urrunetik exekutatzeko aukera emanez. Ahultasun horretarako, CVE-2020-25161 identifikatzailea esleitu da.
- R-SeeNet delakoaren web orriak SQL injekzio bat jasan lezake. Horren bidez, urrutiko erasotzaile batek datu-baseetako kontsultak egin litzake eta informazio konfidentziala lortu. Ahultasun horretarako, CVE-2020-25157 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, SCADA, Ahultasuna.

Baimen desegokiaren ahultasuna Bender etxearen COMTRAXX serieko hainbat produktutan

Argitalpen data: 2020/10/19

Garrantzia: Altua

Kaltetutako baliabideak:

COMTRAXX erabiltzen duten gailu guztiak daude ahultasun horren eraginpean. Produktu hauen 4.2.0 bertsioaren aurrekoak:

- COM465IP, B95061065 eta B95061066 agindu-zenbakia;
- COM465IP, B95061060 eta B95061061 agindu-zenbakia;
- COM465ID, B95061070 agindu-zenbakia;
- CP700, B95061030 agindu-zenbakia;
- CP907, B95061080 agindu-zenbakia;
- CP915, B95061081, B95061085 eta B95061092 agindu-zenbakia.

Azalpena:

Maxim Rupp ikertzaileak, erakundeak koordinatuta, baimen desegokiko ahultasun bat antzeman du Benderren COMTRAXX serieko produktuetan. Fabrikatzaileari horren berri eman dio.

Konponbidea:

4.2.0 bertsiora eguneratzea.

Xehetasunak:

Erabiltzailearen baimena balioztatuta dago sistemaren ibilbide gehienetarako, baina ez guztietarako. Ibilbideei buruzko ezagutzak dituen erasotzaile batek konfigurazio-datuak irakurri eta idatz litzake aurretiko baimenik gabe, kredentzialen egiaztatzea omitituz. Ahultasun horretarako, CVE-2019-19885 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, Ahultasuna.

Baimen desegokia Hitachi ABB Power Grids markaren XMC20 Multiservice-Multiplexer sisteman

Argitalpen data: 2020/10/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- XMC20 R4 eta COGE5 erabiliz, co5ne_r1h07_12.esw aurreko bertsioak;
- XMC20 R6 eta COGE5 erabiliz, co5ne_r2d14_03.esw aurreko bertsioak;

Azalpena:

Hitachi ABB Power Grids etxeak larritasun kritikoko ahultasun baten berri eman du, baimen desegokiaren motakoa.

Konponbidea:

- XMC20 R4: COGE5 co5ne_r1h07_12.esw bertsiora edo osteko batera eguneratzea;
- XMC20 R6: COGE5 co5ne_r2d14_03.esw bertsiora edo osteko batera eguneratzea.

Xehetasunak:

Erasotzaile batek ahultasun hori baliatu lezake, kaltetutako produktuen liburutegi batean dagoena, XMC20 nodora bereziki diseinatutako mezu bat bidaliz, egiaztatu beharrik gabe komunikazio bide bat irekitzeko. Horrek baimenik gabeko sarbidea eragingo luke. Ahultasun horretarako, CVE-2018-10933 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Bufferrak gainezka egitea Rockwell Automation erakundearen 1794-AENT Flex I/O Series B sisteman

Argitalpen data: 2020/10/21

Garrantzia: Altua

Kaltetutako baliabideak:

Ethernet/IP 1794-AENT Flex I/O Series B egokigailua, 1794-AENT Flex I/O, Series B, 4.003 bertsioa eta aurrekoak.

Azalpena:

Cisco Talos enpresako Jared Rittle ikertzaileak larritasun handiko ahultasun honen berri eman dio Rockwell Automation erakundeari. Horren bidez, kodearen urrutiko exekuzioa eragin daiteke.

Konponbidea:

Rockwell Automation erakundeak segurtasun kontrolen erabilera eta sareko segmentazio egokia gomendatzen ditu.

Xehetasunak:

Ethernet/IP Request Path Port Segment, Ethernet/IP Request Path Logical Segment eta Ethernet/IP Request Path Data Segment eremuetan bufferrak gainezka eginez gero, baimenik gabeko urrutiko erasotzaile batek pakete maltzur bat bidal lezake eta horrek gailuaren zerbitzuaren ukapena eragin lezake. Ahultasun horietarako CVE-2020-6083, CVE-2020-6084 eta CVE-2020-6086 identifikatzaileak esleitu dira.

Etiketak: Azpiegitura kritikoak, Ahultasuna

Hainbat ahultasun B. Braun Melsungen produktu batzuetan

Argitalpen data: 2020/10/23

Garrantzia: Handia

Kaltetutako baliabideak:

- OnlineSuite AP, 3.0 bertsioa eta aurrekoak;
- SpaceCom, software U61 bertsioa eta aurrekoak (Estatu Batuetan), eta L81 eta aurrekoak (Estatu Batuetatik kanpo);
- Battery Pack SP Wi-Fiarekin, software U61 bertsioa eta aurrekoak (Estatu Batuetan), eta L81 eta aurrekoak (Estatu Batuetatik kanpo);
- Data module compactplus, software A10 eta A11 bertsioak (ez dira banatzen Estatu Batuetan).

Azalpena:

Hainbat erakundetako ikertzaileek, BSI ManiMed proiektuaren baitan lanean, 14 ahultasunen berri eman dute. 6 larritasun handikoak dira, 7 tartekoak eta bat baxukoa. Motak: direktorio mugatu baterako sarbidearen mugatze desegokia (*relative path transversal*), kontrolatu gabeko bilaketa-ibilbidearen elementua, Excel makroen injekzioa, XSS, birbideratze irekia, XPath injekzioa, saioaren finkapena, salt gabeko norabide bakarreko *hash* baten erabilera, sinadura kriptografikoaren egiaztatze desegokia, pribilegioen kudeaketa desegokia, pasahitz barneratuen erabilera, *debugear* kode aktiboa, eta sarbide kontrol

desegokia.

Konponbidea:

Fabrikatzaileak honako bertsioetara eguneratzea gomendatzen du, azaldutako ahultasunak konpontzeko:

- OnlineSuite Field Service Information, AIS06/20 bertsioa;
- SpaceCom, U62 bertsioa edo ostekoak (Estatu Batuak), eta L82 edo ostekoak (Estatu Batuetatik kanpo);
- Battery Pack SP Wi-Fiarekin, U62 bertsioa edo ostekoak (Estatu Batuetan), eta L82 edo ostekoak (Estatu Batuetatik kanpo);
- Data module compactplus, A12 bertsioa edo ostekoak.

Xehetasuna:

- Direktorio mugatu baterako sarbide-ibilbidearen mugatze desegokiaren ahultasunaren bide (relative path transversal), baimenik gabeko erasotzaile batek artxibo arbitrarioak kargatu eta deskargatu litzake. Ahultasun horretarako, CVE-2020-25172 identifikatzailea esleitu da.
- DLL bahiketaren (hijacking) ahultasun baten bidez, tokiko erasotzaile batek kodea exekutatuko luke sisteman, pribilegio handiko erabiltzaile baten moduan. Ahultasun horretarako, CVE-2020-25174 identifikatzailea esleitu da.
- XSS islatuaren ahultasun baten bidez, urrutiko erasotzaile batek web kode arbitrarioa edo HTML injektatu lezake hainbat kokapenetan. Ahultasun horretarako, CVE-2020-25158 identifikatzailea esleitu da.
- XPath injekzioko ahultasun baten bidez, urrutiko erasotzaile batek, baimenik gabe, informazio sentikorra eskuratu lezake, eta pribilegioak handitu. Ahultasun horretarako, CVE-2020-25162 identifikatzailea esleitu da.
- Direktorio mugatu baterako sarbide-ibilbidearen mugatze desegokiaren ahultasunaren bidez (relative path transversal), zerbitzuaren erabiltzaile pribilegioak dituen erasotzaile batek artxibo arbitrarioak kargatu eta deskargatu litzake bereziki diseinatutako .tar baten bidez. Ahultasun horretarako, CVE-2020-25150 identifikatzailea esleitu da.
- Depurazio kode aktiboaren bidez, material kriptografikoa duen erasotzaile bat root gisa sar liteke gailura. Ahultasun horretarako, CVE-2020-25156 identifikatzailea esleitu da.

Tarteko larritasun eta larritasun baxuko gainerako ahultasunetarako, honako identifikatzaileak esleitu dira: CVE-2020-25170, CVE-2020-25154, CVE-2020-25152, CVE-2020-25164, CVE-2020-25166, CVE-2020-16238, CVE-2020-25168 eta CVE-2020-25160.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Osasuna, Ahultasuna.

Hainbat ahultasun SHUN HU Technology etxearen JUUKO Industrial Radio Remote Control sisteman

Argitalpen data: 2020/10/28

Garrantzia: Altua

Kaltetutako baliabideak:

JUUKO Industrial Radio Remote Control K-800 eta K-808, honela bukatzen diren zenbakien aurreko firmware bertsioekin: 9A, 9B, 9C, eta abar. Zalantzarik izatekotan, SHUN HU Technology laguntza teknikoa.

Azalpena:

Marco Balduzzi, Philippe Z Lin, Federico Maggi, Jonathan Andersson, Akira Urano, Stephen Hilt eta Rainer Vosseler ikertzaileek, Trend Microren ZID erakundearekin elkarlanean, larritasun handiko 2 ahultasunen berri eman dute. Motak: kaptura/erreprodukzioagatiko egiaztatzea eta komando injekzioa.

Konponbidea:

SHUN HU Technology erakundeak bi firmware bertsio berri argitaratu ditu. Ahultasun horiek arintzen dituzte eta erabiltzaileei gomendatzen zaie salmenta-ordezkari batekin edo laguntza teknikoarekin harremanetan jartzeko, eguneratze horien inguruko laguntza jasotzeko.

Xehetasunak:

- K-800 komandoen erreprodukzio eta faltsutze eraso (authentication bypass by capture-replay) baten mende egon daiteke, eta, horren bidez, erasotzaile batek komandoak erreproduzitu litzake, gailua kontrolatu, komandoak ikusi, edo gailu batek funtzionatzeari uztea eragin. Ahultasun horretarako, CVE-2018-17932 identifikatzailea esleitu da.
- Erasotzaile batek bereziki diseinatutako pakete bat sortu lezake komando arbitrario bat kodetzeko, eta K-808 eremuan exekutatu liteke. CVE-2018-19025 identifikatzailea esleitu da ahultasun horretarako.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, Ahultasuna

---

Zerbitzuaren ukapen motako ahultasuna WAGOren hainbat PLC familiatan

Argitalpen data: 2020/10/28

Garrantzia: Altua

Kaltetutako baliabideak:

- 750-352,

- 750-831/xxx-xxx,
- 750-852,
- 750-880/xxx-xxx,
- 750-881,
- 750-889.

FW1etik FW10era arteko firmware bertsioak kaltetuta daude. 2017ko abenduan abiatutako FW11tik aurrerako bertsioak ez daude kaltetuta.

Azalpena:

William Knowles (Applied Risk) ikertzaileak ahultasun baten berri eman dio WAGOri, erakundeak koordinatuta. Horren bidez, erasotzaile batek zerbitzuaren ukapena eragin lezake.

Konponbidea:

Gailua azken firmware bertsiora eguneratzea.

Xehetasunak:

Erasotzaile batek gailua blokeatu lezake HTTP (S) 80/443 portuetara bereziki diseinatutako paketeak bidaliz. CVE-2020-12516 identifikatzailea esleitu da ahultasun horretarako.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun Mitsubishi Electric etxearen produktu batzuetan

Argitalpen data: 2020/10/30

Garrantzia: Kritikoa

Kaltetutako baliabideak:

MELSEC iQ-R sistemaren honako bertsioak daude kaltetuta:

- R 00/01/02 CPU, 20 firmware bertsioa eta aurrekoak;
- R 04/08/16/32/120 (EN) CPU, 52 firmware bertsioa eta aurrekoak;
- R 08/16/32/120 SFCPU, 22 firmware bertsioa eta aurrekoak;
- R 08/16/32/120 PCPU, bertsio guztiak;
- R 08/16/32/120 PSFCPU, bertsio guztiak;
- R 16/32/64 MTCPU, bertsio guztiak.

MELSEC iQ-R Series modulu hauek daude kaltetuta:

- EtherNet/IP Network Interface Module, RJ71EIP91: serie zenbakiaren lehenengo 2 digituak 02 edo aurrekoak badira;
- PROFINET IO Controller Module, RJ71PN92: serie zenbakiaren lehenengo bi digituak 01 edo aurrekoak badira;
- High Speed Data Logger Module, RD81DL96: serie zenbakiaren lehenengo 2 digituak 08 edo aurrekoak badira;
- MES Interface Module, RD81MES96N: serie zenbakiaren lehenengo 2 digituak 04 edo aurrekoak badira;
- OPC UA Server Module, RD81OPC96: serie zenbakiaren lehenengo 2 digituak 04 edo aurrekoak badira.

MELSEC Q Series sistemaren honako bertsioak daude kaltetuta:

- Q 03 UDECPU, Q 04/06/10/13/20/26/50/100 UDEHCPU, 22081 serie zenbakia eta aurrekoak;
- Q 03/04/06/13/26 UDVCPU, 22031 serie zenbakia eta aurrekoak;
- Q 04/06/13/26 UDVCPU, 22031 serie zenbakia eta aurrekoak;
- Q 172/173 DCPU Q 172/173 DCPU-S1era arte, bertsio guztiak;
- Q 172/173 DSCPU, bertsio guztiak;
- Q 170 MCPU, bertsio guztiak;
- Q 170 MSCPU, Q 170 MSCPU (-S1) arte, bertsio guztiak;
- RJ-ME100, bertsio guztiak.

MELSEC L Series sistemaren honako bertsioak daude kaltetuta:

- L 02/06/26 CPU (-P), L 26 CPU - (P) BT, bertsio guztiak.

Azalpena:

Mitsubishi Electric etxeak 7 ahultasunen berri eman dio CISAri: 2 larritasun kritikokoak, 4 handikoak eta bat tartekoa. Motak: operazioen mugatze okerra memoria bufferraren mugen barruan, sarbide desegokiaren kontrola, saioaren finkapena, erakusle baliogabearen erreferentzia galtzea, argudioaren injekzioa eta baliabideen kudeaketa akatsak.

Konponbidea:

Fabrikatzailearen countermeasures atalean fabrikatzailearen bi abisuak begiratzea (2020-012_en y 2020-013_en) dagozkion eguneratzeak aplikatzeko.

Xehetasunak:

Larritasun kritikoko ahultasunen bidez, baimenik gabeko urrutiko erasotzaile batek produktuen funtzioak geldiaraz litzake, edo programa maltzur bat exekutatu, bereziki diseinatutako pakete baten bidez. Ahultasun horietarako CVE-2020-5653 eta CVE-2020-5656 identifikatzaileak esleitu dira.

Gainerako ahultasunetarako, honako identifikatzaileak esleitu dira: CVE-2020-5654, CVE-2020-5655, CVE-2020-5657, CVE-2020-5652 eta CVE-2020-5658.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna