2020ko Azaroaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Hainbat ahultasun NEXCOM NIO 50 sisteman

Argitalpen data: 2020/11/04

Garrantzia: Ertaina

Kaltetutako baliabideak:

NEXCOM NIO 50, bertsio guztiak.

Azalpena:

Zero Day Initiative erakundeak tarteko larritasuneko bi ahultasunen berri eman du. Motak: sarrera-datuen balioztatze okerra eta informazio sentikorreko testu argiaren transmisioa.

Konponbidea:

NEXCOM erakundeak dagoeneko ez du NIO 50 saltzen ez mantentzen, eta bizitza erabilgarriaren amaiera gertu duen produktutzat dauka.

Xehetasunak:

- Kaltetutako produktuak ez du sarbidea behar den moduan balioztatzen, eta, horren ondorioz, erasotzaile batek zerbitzuaren ukapen motako (DoS) eraso bat burutu lezake. Ahultasun horretarako, CVE-2020-25151 identifikatzailea esleitu da.
- Kaltetutako produktuak informazio konfidentzial zifratua transmititzen du. Horren ondorioz, erasotzaile batek informazio hori eskuratu lezake. Ahultasun horretarako, CVE-2020-25155 identifikatzailea esleitu da.

Etiketak: Azpiegitura kritikoak, Ahultasuna

Hainbat ahultasun Moxaren MXview Series sisteman

Argitalpen data: 2020/11/05

Garrantzia: Kritikoa

Kaltetutako baliabideak:

MXview Series, 3.0 firmware bertsiotik 3.1.8 bertsiora artekoak.

Azalpena:

Cisco Talos erakundeko Yuri Kramarz-ek larritasun kritikoko hainbat ahultasunen berri eman dio Moxari. Mota: berezko baimen okerrak.

Konponbidea:

Software berria deskargatzea, segurtasun-kopien eta migrazioaren prozedura jarraitzea, MXview eguneratzeko.

Prozesu horretan zehar arazorik baduzu, Moxaren talde teknikoarekin jar zaitezke harremanetan.

Xehetasunak:

Erasotzaile batek iturri-artxibo bat editatu lezake bereziki diseinatutako kodea sartzeko eta pribilegioetan gora egitea lortzeko. Ahultasun horietarako, CVE-2020-13536 eta CVE-2020-13537 identifikatzaileak erreserbatu dira.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Bufferrak gainezka egitea WECON erakundearen PLC Editor sisteman

Argitalpen data: 2020/11/06

Garrantzia: Altua

Kaltetutako baliabideak:

- PLC Editor, 1.3.8 bertsioa eta aurrekoak.

Azalpena:

Natnael Samson eta Francis Provencher ikertzaileek, Trend Micro's Zero Day Initiative erakundearekin batera, larritasun handiko ahultasun horien berri eman diote CISAri.

Konponbidea:

WECON konponbide bat garatzen ari da. Informazio gehiago lortzeko, WECONekin harremanetan jar zaitezke web atariaren bidez .

Xehetasunak:

- Pilan oinarritutako bufferraren gainezkatze motako ahultasun baten ondorioz (stack), erasotzaile batek kodearen exekuzio arbitrarioa burutu lezake. Ahultasun horretarako, CVE-2020-25177 identifikatzailea esleitu da.
- Heap eremuko bufferraren gainezkatze motako ahultasun baten ondorioz (stack), erasotzaile batek kodearen exekuzio arbitrarioa burutu lezake. Ahultasun horretarako, CVE-2020-25181 identifikatzailea esleitu da.

Etiketak: Azpiegitura kritikoak, Ahultasuna

Hainbat ahultasun Mitsubishi Electric GT14 sistemaren GOT2000 serieetan

Argitalpen data: 2020/11/06

Garrantzia: Kritikoa

Kaltetutako baliabideak:

CoreOS daukaten honako GOT1000 ereduak, 05.65.00.BD bertsioa eta aurrekoak, kaltetuta daude:

- GT1455-QTBDE,
- GT1450-QMBDE,
- GT1450-QLBDE,
- GT1455HS-QTBDE,
- GT1450HS-QMBDE.

Azalpena:

Mitsubishi Electric etxeak 6 ahultasunen berri eman dio CISAri; 2 larritasun kritikokoak, 3 altukoak 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 2020-014_en oharrean azaldutakoaren arabera, Core OS 05.76.00.BG bertsiora eta ostekoetara egokitzea (MELSOFT GT Designer3 Version1 [GOT1000], 1.245F bertsioa eta ostekoak).

Xehetasunak:

Larritasun kritikoko ahultasunak ondoren azalduta daude:

- Kaltetutako produktuak memoriaren korrupzio ahultasun bat dauka, eta, horren ondorioz, erasotzaile batek bereziki diseinatutako pakete bat bidal lezake, eta horrek zerbitzuaren ukapena (DoS) edo kodearen exekuzioa eragin litzake. Ahultasun horretarako, CVE-2020-5644 identifikatzailea esleitu da.
- Kaltetutako produktuak sarbide kontrolaren arazo bat dauka, eta horren ondorioz erasotzaile batek bereziki diseinatutako pakete bat bidal lezake, eta horrek zerbitzuaren ukapena (DoS) edo kodearen exekuzioa eragin litzake. Ahultasun horretarako, CVE-2020-5647 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak esleitu dira: CVE-2020-5645, CVE-2020-5646, CVE-2020-5648 eta CVE-2020-5649.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun KUKA etxearen Visual Components sisteman

Argitalpen data: 2020/11/09

Garrantzia: Altua

Kaltetutako baliabideak:

Visual Components Network License Server, 2.0.8. bertsioa.

Azalpena:

Sharon Brizinov, Claroty enpresako segurtasun-ikertzaileak, larritasun handiko 2 ahultasun antzeman ditu. Motak: baimenik gabeko erabiltzaile bati informazio konfidentziala erakustea eta antzeman gabeko salbuespena.

Konponbidea:

CVE-2020-10292 identifikatzailea duen ahultasunerako, mitigazio neurri moduan, honakoa gomendatzen da: Visual Components ez abiaraztea LAN edo WAN konexioa duenean, eta birtualizazioaren bidez simulazioari eustea. Beste ahultasunerako, ez da mitigazio-neurririk aportatzen.

Xehetasunak:

- Protokoloak zerbitzari jasotzaileari buruzko informazioa eta lizentziaren eta lizentzien kudeaketaren informazioa filtratzen du, beste batzuen artean. Ahultasun honen bidez, erasotzaile batek KUKA simulazio sistema baten inguruko informazioa berreskura lezake, bereziki, simulagailura konektatuta dagoen lizentzien zerbitzari bertsioa. Horrela, antzeko ezaugarriak dituzten tokiko simulazioak abiatuko lituzke, mugimenduaren birtualizazioaren dinamika hobetu ulertuz eta beste eraso batzuk burutzeko aukera irekiz. Ahultasun horretarako, CVE-2020-10291 identifikatzailea esleitu da.
- Protokoloa zerbitzu ukapenaren motako ahultasun baten mende dago (DoS), puntero arbitrario baten deribazio bidez. Ahultasun horren bidez, erasotzaile batek bereziki diseinatutako pakete bat pasa lezake, eta zerbitzuak prozesatzean, pilako puntero arbitrario bat egingo luke, zerbitzua bukaraziko lukeen antzeman gabeko salbuespen bat eraginez. Ahultasun horretarako, CVE-2020-10292 identifikatzailea esleitu da.

Etiketak: Azpiegitura kritikoak, Birtualizazioa, Ahultasuna.

Oracle WebLogic Server sistemako ahultasunak Control Industrial erakundeko sistemei eragin die

Argitalpen data: 2020/11/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Fabrikatzaile batzuek Oracle WebLogic Server erabiltzen dute produktu eta konponbideetan, beraz, kaltetu egin dira.

- Philips produktuak:
  - Tasy EMR v12.2.1.3.

Azalpena:

Ahultasun hori erraz baliatu daiteke, eta baimenik gabeko erasotzaile batek, HTTP bidezko sarbidearekin, Oracle WebLogic Server konprometitu lezake, Control Industrial sistemetan erabilia. Abisu hori INCIBE-CERT bidez argitaratu zen, Oracle WebLogic Server-eko urrutiko exekuzio motako ahultasun gisa.

Konponbidea:

Partxeen Fusion Middleware (login) dokumentuan azaldutako jarraibideei kasu egitea.

Xehetasunak:

Ahultasun hori CVE-2020-14882 identifikatzailearekin erlazionatua dago, eta Oracleren eguneraketa kritikoen artean (octubre 2020) jaso zen. Horren bidez, baimenik gabeko erasotzaile batek, HTTPren bidez sarera sartuta, Oracle WebLogic Server sistema konprometitu dezake. Urrunetik baliatu daiteke, erabiltzailerik edota pasahitzik gabe. Ahultasun horretarako, CVE-2020-14750 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Java, Oracle, Osasungintza, Ahultasuna

Siemens segurtasun oharrak, 2020ko azaroa

Argitalpen data: 2020/11/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SCALANCE W1750D, bertsio guztiak;
- SIMATIC S7-300 CPU familia (erlazionatutako CPU ET200 eta SIPLUS aldagaiak barne), bertsio guztiak;
- SINUMERIK 840D sl, bertsio guztiak.

Azalpena:

Siemensek produktu batzuen inguruan hainbat segurtasun-eguneratze argitaratu ditu, bere hileroko jakinarazpenean.

Konponbidea:

- SCALANCE W1750D azken firmware bertsiora eguneratzea, eta Control Plane Security Best Practices eremuan azaldutako jarraibideak kontuan hartzea. Sarearen konfigurazioaren eta arriskuarekiko tolerantziaren arabera, baliteke ekintzarik behar ez izatea.
- SIMATIC S7-300 CPU eta SINUMERIK 840D sl familien 102/tcp portutik sarerako sarbidea babestea.

Xehetasunak:

Siemensek, segurtasun partxeei buruzko hileroko jakinarazpenean, 6 segurtasun-abisu eman ditu; horietatik 4 aurretik argitaratutako abisuen eguneratzeak dira.

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Sarbide okerraren balioztatze motako ahultasun 1;
- Baliabideen kontrolik gabeko kontsumoaren motako ahultasun 1;

Ahultasun horietarako, honako identifikatzaileak erreserbatu dira: CVE-2016-2031 eta CVE-2020-15783.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Siemens, Ahultasuna.

Schneider Electric erakundearen produktuen ahultasunak

Argitalpen data: 2020/11/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- M340 CPUs:
  - BMX P34x, bertsio guztiak.
- M340 Communication Ethernet moduluak:
  - BMX NOE 0100 (H), bertsio guztiak;
  - BMX NOE 0110 (H), bertsio guztiak;
  - BMX NOC 0401, bertsio guztiak;
  - BMX NOR 0200H, bertsio guztiak.
- Ethernet COPRO integratua duten premium prozesatzaileak:
  - TSXP574634, TSXP575634 y TSXP576634, bertsio guztiak.
- Premium komunikazio moduluak:
  - TSXETY4103, bertsio guztiak;
  - TSXETY5103, bertsio guztiak.
- Ethernet COPRO integratua duten quantum prozesatzaileak:
  - 140CPU65xxxxx, bertsio guztiak.
- Quantum komunikazio moduluak:
  - 140NOE771x1, bertsio guztiak;
  - 140NOC78x00, bertsio guztiak;
  - 140NOC77101, bertsio guztiak.
- EcoStruxure™ Operator Terminal Expert Runtime 3.1 Service Pack 1A eta hauetan instalatutako aurrekoak:
  - Windows PC, legacy moduan BIOS erabiliz;
  - Harmony iPC (HMIG5U, HMIG5U2) legacy moduan BIOS erabiliz.
- IGSS Definition (Def.exe), 14.0.0.20247 bertsioa eta aurrekoak.
- EcoStruxure Building Operation:
  - WebReports, 1.9tik 3.1era bitarteko bertsioak;
  - WebStation, 2.0tik 3.1era bitarteko bertsioak;
  - Enterprise Server instalatzailea, 1.9tik 3.1era bitarteko bertsioak;
  - Enterprise Central instalatzailea, 2.0tik 3.1era bitarteko bertsioak;
- Modicon M221, erreferentzia guztiak bertsio guztietan.
- Easergy T300, 2.7 firmware bertsioa eta aurrekoak.
- PLC Simulator, EcoStruxureTM Control Expert-erako, bertsio guztiak.
- PLC Simulator, Unity Pro-rako (lehen EcoStruxureTM Control Expert deitzen zen), bertsio guztiak.

Azalpena:

Schneider Electric erakundeak hainbat ahultasunen berri eman du: 3 larritasun kritikokoak, 16 handikoak, 9 tartekoak eta 2 baxukoak.

Konponbidea:

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

Xehetasunak:

Larritasun kritikoko ahultasunak ondoren azalduta daude:

- Sarbide kontrol desegokiaren motako ahultasun bat dago, eta horrek arazo ugari sor ditzake. Horien artean daude informazioa erakusgai geratzea, zerbitzu ukapena (DoS) eta komandoen exekuzioa erasotzaile baten sarbidea ez dagoenean mugatuta edo behar ez den moduan mugatuta dagoenean. Ahultasun horretarako, CVE-2020-7561 identifikatzailea esleitu da.
- Buffer klasikoaren gainezkatze motako ahultasun bat dago, eta horrek EcoStruxure TM Control Expert softwarean dagoen PLC simulagailua blokeatu lezake, bereziki diseinatutako eskaera bat Modbus bidez jasotzean. Ahultasun horretarako, CVE-2020-7559 identifikatzailea esleitu da.
- Egiaztatze saiakeren muga desegokiaren motako ahultasun bat dago, eta, horren ondorioz, baimendu gabeko komandoak exekuta litezke, Modbus bidez indarrez eraso bat egiten denean. Ahultasun horretarako, CVE-2020-28212 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak esleitu dira: CVE-2020-7562, CVE-2020-7563, CVE-2020-7564, CVE-2020-7544, CVE-2020-7550, CVE-2020-7551, CVE-2020-7552, CVE-2020-7553, CVE-2020-7554, CVE-2020-7555, CVE-2020-7556, CVE-2020-7557, CVE-2020-7558, CVE-2020-7569, CVE-2020-7570, CVE-2020-7571, CVE-2020-7572, CVE-2020-28209, CVE-2020-28210, CVE-2020-7565, CVE-2020-7566, CVE-2020-7567, CVE-2020-7568, CVE-2020-7538, CVE-2020-28211 eta CVE-2020-28213.

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

Hainbat ahultasun OSIsoft produktuetan

Argitalpen data: 2020/11/11

Garrantzia: Altua

Kaltetutako baliabideak:

- OPC XML-DA 1.7.3.x sistemarako PI Interface bertsioaren aurrekoak.
- PI Vision 2020 bertsioaren aurrekoak.

Azalpena:

OSIsoft produktuei eragiten dieten larritasun handiko eta tarteko bi ahultasun identifikatu dira. Erasotzaile batek ahultasun horiek baliatu litzake kode arbitrarioaren injekzioa egiteko edo baimenik gabeko informazioa erakusteko.

Konponbidea:

Kaltetutako produktuen azken bertsiora eguneratzea:

- OPC XML-DA 1.7.3.x sistemarako PI Interface.
- PI Vision 2020 3.5.0.

Xehetasunak:

OPC XML-DA sistemarako PI Interface produktuari eragiten dion larritasun handiko ahultasun bat antzeman da. Horren ondorioz, erasotzaile batek kode arbitrarioa exekuta lezake urrunetik, OPC XML-DA zerbitzaria kontrolatuta. Ahultasun horretarako, CVE-2013-0006 identifikatzailea esleitu da.

Larritasun handiko beste ahultasunetako batek PI Vision produktuari eragiten dio, eta PI ProcessBook artxiboetarako idazketa sarbidea duen erasotzaile batek kodea exekuta lezake urrunetik, PI Vision sistemara inportatuz. Ahultasun horretarako, CVE-2020-25163 identifikatzailea esleitu da.

Tarteko larritasuna duen ahultasunerako CVE-2020-25167 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasunak.

Kontrolik gabeko baliabideen kontsumoa Mitsubishi Electric MELSEC iQ-R Series sisteman

Argitalpen data: 2020/11/13

Garrantzia: Tartekoa

Kaltetutako baliabideak:

Mitsubishi Electric erakundeak jakinarazi du ahultasun batek MELSEC iQ-R seriearen CPU moduluak kaltetu dituela:

- R00/01/02 CPU, 05etik 19ra arteko *firmware* bertsioak;
- R04/08/16/32/120(EN) CPU, 35etik 51ra arteko *firmware* bertsioak.

Azalpena:

Xiaofei.Zhang txinatar ikertzaileak tarteko larritasuneko ahultasun baten berri eman du. Mota: kontrolik gabeko baliabide kontsumoa.

Konponbidea:

Fabrikatzaileak honako *firmware* bertsioetara eguneratzea gomendatzen du, azaldutako ahultasuna konpontzeko:

- R00/01/02 CPU, 20 *firmware* bertsioa edo ostekoak;
- R04/08/16/32/120(EN) CPU, 52 *firmware* bertsioa edo ostekoak.

Xehetasuna:

Zerbitzu ukapenaren motako (DoS) ahultasun bat dago, MELSEC iQ-R serieko CPU moduluen kontrolik gabeko baliabide kontsumoaren ondorioz. Ahultasun horrek ez die produktuei eragiten CPUaren moduluen *To Use or Not to* Use Web Server parametroa *Not Use* gisa konfiguratzen bada. Hori da berezko konfigurazioa. Ahultasun horretarako, CVE-2020-5666 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Baimen desegokia Becton, Dickinson and Company (BD) produktuetan

Argitalpen data: 2020/11/13

Garrantzia: Handia

Kaltetutako baliabideak:

- BD Alaris PC Unit, Model 8015, 9.33.1 bertsioa eta aurrekoak;
- BD Alaris Systems Manager, 4.33 bertsioa eta aurrekoak.

Azalpena:

Medigate etxeak larritasun handiko ahultasun horren berri eman dio BDri. Mota: baimen desegokia. Horren bidez, erasotzaile batek zerbitzu ukapena eragin lezake.

Konponbidea:

BDk honako arintzeak eman ditu:

- BD zerbitzariaren eguneratze arrunten barruan, Systems Manager instalazio asko eguneratu egin dira dagoeneko, ahultasun hori konpontzeko.
- BD etxeak BD Alaris PC Unit softwarearen hurrengo bertsioa bat abiaraztea pentsatu du, BD Alaris Systems Manager sistemaren 12.0.1, 12.0.2, 12.1.0 eta 12.1.2 bertsioetarako.
- Systems Manager zerbitzarian firewall delakoa gaitzea eta portu eta zerbitzuen bidezko murrizketei buruzko arauak ezartzea, BD produktuaren segurtasun-dokumentu teknikoaren arabera.

Informazio gehigarria lortzeko, kontsultatu BD produktuaren segurtasun-buletina.

Xehetasuna:

Sarearen saioko baimen desegokiaren motako ahultasun baten bidez, BD Alaris PC Unit eta BD Alaris Systems Manager bertsio espezifikoen arteko egiaztatze prozesu baten barruan, erasotzaile batek zerbitzu-ukapena eragin lezake PC BD Alaris unitatean, bidean dauden datuen goiburuak aldatuz. Horren ondorioz, PC BD Alaris unitatearen haririk gabeko gaitasuna erori egingo litzateke, eta PC unitatearen eskuzko funtzionamendua ekarriko luke. Ahultasun horretarako, CVE-2020-25165 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Osasuna, Ahultasuna.

Hainbat ahultasun Paradox IP150-en

Argitalpen data: 2020/11/18

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Paradox IP150, firmwarearen 5.02.09 bertsioa.

Azalpena:

Microsofteko Omri Ben-Bassat ikertzaileak 2 ahultasunen berri eman du, bat larritasun kritikokoa eta bestea altukoa, pilan (stack) oinarritutako bufferraren gainezkatze eta bufferraren gainezkatze klasiko erakoak.

Konponbidea:

Arintze neurrien xehetasunak eskuratzeko Paradox-en zerbitzuarekin harremanetan jarri beharra dago emailera idatziz.

Xehetasunak:

- Kaltetutako produktua ahula da pilan (stack) oinarritutako 3 buffer gainezkatzeren aurrean. Hori baliatuz autentifikatu gabeko erasotzaile batek kode arbitrarioa exekuta lezake urrunetik. Larritasun kritikoko ahultasun horretarako CVE-2020-25189 identifikatzailea erabili da.
- Kaltetutako produktua ahula da autentifikazioaren ondoreneko 5 buffer gainezkatzeren aurrean (bufferraren

gainezkatze klasiko modura ezaguna). Hori baliatuz saioa hasi duen erabiltzaile batek kode arbitrarioa exekuta lezake urrunetik. Larritasun altuko ahultasun horretarako CVE-2020-25185 identifikatzailea erabili da.

Etiketak: Komunikazioak, Azpiegitura kritikoak, Ahultasuna

Baimen desegokia egiaztatzea Johnson Controls enpresaren victor Web Client sisteman

Argitalpen data: 2020/11/18

Garrantzia: Handia

Kaltetutako baliabideak:

- Victor Web Client, 5.6 bertsioa eta aurrekoak;
- C ? CURE Web Client, 2.90 bertsioa eta aurrekoak

Webgunean oinarritutako C ? CURE 9000 bezero berria, C ? CURE 9000 v2. 90 sisteman sartu zena, ez da kaltetu.

Azalpena:

Joachim Kerschbaumer ikertzaileak baimen desegokiaren motako ahultasun baten berri eman dio Johnson Controls konpainiari.

Konponbidea:

- victor Unified Client v5.6 SP1;
- Web Client_c2.70_5.2_Update02;
- Web Client_c2.80_v5.4.1_Update04;
- CCureWeb_2.90_Update01.

Xehetasuna:

Baimen desegokiaren egiaztatze arloko ahultasun baten ondorioz, baimenik gabeko erasotzaile batek bere token web JSON propioa sortu eta sinatu lezake, eta API http metodo bat exekutatzeko erabili, baimen baliagarririk gabe. Zirkunstantzia batzuetan, horrek sistemaren erabilgarritasunari eragin ahal dio, zerbitzu ukapenaren motako eraso baten bidez. Ahultasun horretarako, CVE-2020-9049 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Bufferraren gainezkatze erako ahultasuna Real Time Automation-en (RTA) EtherNet/IP-n

Argitalpen data: 2020/11/18

Garrantzia: Kritikoa

Kaltetutako baliabideak:

499ES EtherNet/IP Adaptor Source Code-ren 2.28 bertsioa baino lehenagokoak, bere TCP/IP pilan.

Azalpena:

Claroty-ko Sharon Brizinov ikertzaileak bufferraren gainezkatze erako ahultasun bat aurkitu du memoriaren stack eskualdean. Hori baliatuz, urruneko erasotzaile batek kaltetutako gailuan zerbitzuaren ukapen egoera edo kodearen urruneko exekuzioa eragin litzake.

Konponbidea:

Real Time Automation-en laguntza zerbitzuarekin harremanetan jartzea gomendatzen da.

Horrez gain, honako arintze neurri hauek ezartzea gomendatzen da:

- Gailu guztiek sarera duten agerpena ahalik eta gehien murriztea.
- Kontrol industrialeko sistemak firewall-en atzean kokatzea eta enpresa edo kudeaketa saretik isolatzea.
- Urruneko sarbidea behar denean metodo seguruak erabiltzea, esate baterako sare pribatu birtualak (VPN).

Xehetasunak:

Real Time Automation-en EtherNet/IP-n aurkitutako ahultasuna baliatuz bufferraren gainezkatzea eragin liteke memoriaren stack eskualdean, bereziki diseinatutako pakete bat bidaliz. Horrek zerbitzuaren ukapena (DoS) edo kodearen exekuzioa (RCE) eragin litzake.

Ahultasun horretarako CVE-2020-25159 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak, Azpiegitura kritikoak, IoT, SCADA, Ahultasuna

---

Pribilegioen eskalatze erako ahultasuna Beckhoff-en TwinCAT System Tray-en

Argitalpen data: 2020/11/20

Garrantzia: Altua

Kaltetutako baliabideak:

TwinCAT XAR, modu lehenetsian instalazio bide bat daukaten 3.1 bertsioak.

Azalpena:

Ayushman Dutta ikertzaileak jakinarazi dio TwinCAT XAR-en lehenetsitako instalazioetan ahultasun bat dagoela, zehazki instalazio bidean eta TwinCAT System Tray-ren baimenetan, TcSysUI.exe exekutagarriaren bidez. Ahultasun horren ondorioz, erabiltzaile lokal batek sistema bereko beste erabiltzaile batzuek exekuta ditzaketen exekutagarriak ordeztu edo alda litzake, eta horrela bertan pribilegioen eskalatze bat gertatutako litzateke.

Konponbidea:

TwinCATen instalazioa 'C:/Program Files/TwinCAT' edo 'C:/Programa-fitxategiak/TwinCAT' bidean egitea gomendatzen da.

Programa dagoeneko beste bide batean instalatuta izanez gero, desinstalatzea gomendatzen da, eta aipatutako bide zuzen horretan berriro instalatzea. Horretarako instalazio pertsonalizatua erabili behar da. Hori egin baino lehen gailu osoaren segurtasun kopia bat egitea gomendatzen da, eta ondoren beste bide batzuetan dauden fitxategiak ezabatzea.

Xehetasuna:

Aurkitutako ahultasuna baliatuz sistemako erabiltzaile batek aldaketak egin litzake TwinCATen lehenetsitako "C:/TwinCAT" instalazio bidean erabiltzen diren fitxategi eta programetan, TcSysUI.exe programan barne, sistemaren abioan modu lehenetsian kargatzen dena TwinCat System Tray-rentzat. Hori erabiltzaile administratzaileen kasuan ere gertatzen da eta, ondorioz, administratzaile pribilegiorik gabeko erabiltzaile batek fitxategi horiek aldatzen baditu, pribilegioen igoera egin lezake sisteman administratzaile batek saioa hastean.

Ahultasun horretarako CVE-2020-12510 identifikatzailea erabili da.

Etiketak: Azpiegitura kritikoak, IoT, Ahultasuna, Windows

Hainbat ahultasun Endress Hauser-en hainbat produktutan

Argitalpen data: 2020/11/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- CVE-2020-12495 ahultasunerako:
  - Ecograph T: firmwarearen 1.0.0 (07/2013) bertsioa edo lehenagokoak;
  - Ecograph T Neutral/Private Label; firmwarearen 2.0.0 (08/2015) bertsioa edo lehenagokoak.
- CVE-2020-12496 ahultasunerako, firmwarearen 2.0.0 (08/2015) bertsioa edo lehenagokoak, honako produktu hauetan:
  - Ecograph T,
  - Memograph M,
  - Ecograph T Neutral/Private Label,
  - Memograph M Neutral/Private Label.

Azalpena:

Maxim Rupp ikertzaileak Endress Hauser fabrikatzaileari bi ahultasunen berri eman dio, pribilegioen kudeaketa desegoki erakoa bata, eta bestea, baimendu gabeko erabiltzaile bati informazio konfidentziala erakuste erakoa, hainbat gailuri eragiten dietenak. Fabrikatzaileak, bere aldetik, ahultasun hauen berri eman dio

Konponbidea:

Fabrikatzaileak gomendatzen du bezeroek firewall perimetral bat konfiguratzea sareetako trafikoa eta gailurako konfiantzakoak ez diren erabiltzaileak blokeatzeko. Gomendio hauek gailuaren dokumentazioan jasoko dira (funtzionamendurako jarraibideak). Gainera, operadore, zerbitzu eta administratzaile konturako lehenetsitako pasahitza aldatu beharra dago.

Xehetasunak:

- Kaltetutako gailuak daukan erabiltzailearen web interfazeak daukan sarbide sistema token dinamikoetan oinarritzen da, eta idazketa eta irakurketa pribilegio ezberdinak dituzten rolak esleituta ditu. Ahultasunaren arrazoia da erabiltzaile saioak ez direla zuzen ixten, eta pribilegio gutxiagoko erabiltzaile bati pribilegio altuagoak esleitzen zaizkiola saioa hasten duenean. Larritasun kritikoko ahultasun horretarako CVE-2020-12495 identifikatzailea erabili da.
- Firmwarearen bertsioak token dinamiko bat dauka zerbitzarira bidaltzen duen eskaera bakoitzeko, eta horren ondorioz errepikatutako eskaerak eta analisia aski konplexuak dira. Nolanahi ere, sarbidearen kontrol matrizeak zerbitzariaren aldean zuen arazo bat aurkitu zen. Hori baliatuz pribilegio gutxiko erabiltzaile batek endpoint-en informazioa eskura lezake, baldintza normaletan horietara sarbiderik izango ez lukeenean. Larritasun ertaineko ahultasun horretarako CVE-2020-12496 identifikatzailea erabili da.

Etiketak: Azpiegitura kritikoak, Osasuna, Ahultasuna

Baliabideen kontrolik gabeko kontsumoa Mitsubishi Electric-en MELSEC IQ-R series-en

Argitalpen data: 2020/11/20

Garrantzia: Altua

Kaltetutako baliabideak:

Mitsubishi Electric-ek jakinarazi duenez ahultasunak MELSEC iQ-R serieko CPU moduluen honako produktu hauei eragiten die:

- R00/01/02 CPU, firmwarearen 19. bertsioa eta lehenagokoak;
- R04/08/16/32/120 (EN) CPU, firmwarearen 51. bertsioa eta lehenagokoak;
- R08/1632/120 SFCPU, firmwarearen 22. bertsioa eta lehenagokoak;
- R08/16/32/120 PCPU, bertsio guztiak;
- R08/16/32/120 PSFCPU, bertsio guztiak;
- RJ71EN71, firmwarearen 47. bertsioa eta lehenagokoak;
- RJ71GF11-T2, firmwarearen 47. bertsioa eta lehenagokoak;
- RJ72GF15-T2, firmwarearen 07. bertsioa eta lehenagokoak;
- RJ71GP21-SX, firmwarearen 47. bertsioa eta lehenagokoak;
- RJ71GP21S-SX, firmwarearen 47. bertsioa eta lehenagokoak;
- RJ71C24(-R2/R4), bertsio guztiak;
- RJ71GN11-T2, bertsio guztiak.

Azalpena:

Xiaofei.Zhang-ek ahultasun bat aurkitu du, baliabideen kontrolik gabeko kontsumo erakoa eta larritasun altukoa. Hori baliatuz zerbitzuaren ukapena (DoS) eragin liteke kaltetutako produktuetan.

Konponbidea:

Ahultasun hori konpontzeko fabrikatzaileak firmwarearen honako bertsio hauetara eguneratzea gomendatzen du:

- R00/01/02 CPU, 20. bertsiora edo berriago batera;
- R04/08/16/32/120 (EN) CPU, 52. bertsiora edo berriago batera;
- R08/16/32/120 SFCPU, 23. bertsiora edo berriago batera;
- RJ71EN71, 48. bertsiora edo berriago batera;
- RJ71GF11-T2, 48. bertsiora edo berriago batera;
- RJ72GF15-T2, 08. bertsiora edo berriago batera;
- RJ71GP21-SX, 48. bertsiora edo berriago batera;
- RJ71GP21S-SX, 48. bertsiora edo berriago batera.

Xehetasunak:

Baliabideen kontrolik gabeko kontsumo erako ahultasunak zerbitzuaren ukapen egoera (DoS) eragin lezake MELSEC iQ-R serieko CPU moduluen exekuzioan eta komunikazioan, erasotzaileak bereziki diseinatutako SLMP pakete bat bidali ondoren. Ahultasun horretarako CVE-2020-5668 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak, Azpiegitura kritikoak, Ahultasuna

Ahultasuna Fuji Electric V-Server Lite sisteman

Argitalpen data: 2020/11/25

Garrantzia: Handia

Kaltetutako baliabideak:

V-Server Lite, todas las versiones anteriores a 3.3.24.0.

Azalpena:

VinCSS erakundeko Tran Van Khang-khangkito ikertzaileak, ZDIrekin elkarlanean, mugetatik kanpoko idazketa motako ahultasun baten berri eman du.

Konponbidea:

Softwarea bertsio honetara eguneratzea: 3.3.25.0.

Xehetasunak:

Kaltetutako produktua memoriaren mugetatik kanpoko idazketaren mende egon daiteke; horren ondorioz, erasotzaile batek urrutiko kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE 2020-25171 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.