2021ko urtarrilaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Hainbat ahultasun Pepperl Fusch produktu batzuetan

Argitalpen data: 2021/01/05

Garrantzia: Altua

Kaltetutako baliabideak:

P F Comtrol sistemaren 1.5.48 firmware bertsioak eta aurrekoak:

- IO-Link Master 4-EIP,
- IO-Link Master 8-EIP,
- IO-Link Master 8-EIP-L,
- IO-Link Master DR-8-EIP,
- IO-Link Master DR-8-EIP-P,
- IO-Link Master DR-8-EIP-T,
- IO-Link Master 4-PNIO,
- IO-Link Master 8-PNIO,
- IO-Link Master 8-PNIO-L,
- IO-Link Master DR-8-PNIO,
- IO-Link Master DR-8-PNIO-P,
- IO-Link Master DR-8-PNIO-T.

Azalpena:

SEC Consult Vulnerability Lab erakundeko T.Weber ikertzaileak ahultasun horren berri eman du, erakundeak koordinatuta. Horren bidez, erasotzaile bat gailura eta bertako informaziora sar liteke, edo programak exekutatu.

Konponbidea:

Kaltetutako produktuak honako firmware paketeekin eguneratu:

- U-Boot bootloader, 1.36 bertsioa edo ostekoa;
- System image, 1.52 bertsioa edo ostekoa;
- Application base, 1.6.11 edo ostekoa.

Gainera, sare publiko batera konektatutako produktuetarako, fabrikatzaileak honakoa gomendatzen du:

- Kanpo-babeserako neurriak praktikan jartzea.
- Firewall baten bidez gailurako konfiantzazkoak ez diren sareen trafikoa blokeatu behar da, bereziki administrazio webgunera zuzendutako trafikoari dagokionez.
- Gailuaren erabiltzaile kontuak pasahitz seguruen bidez babestu behar dira.
- Pertsona edo aplikazio ez fidagarriak sar badaitezke gailua konektatuta dagoen sarera, hiru erabiltzaile kontuen pasahitzak konfiguratzea gomendatzen da.

Xehetasunak:

Identifikatutako ahultasun motak honakoak dira:

- Cross-Site Request Forgery (CSRF). Larritasun handiko ahultasun horretarako CVE-2020-12511 identifikatzailea esleitu da.
- Cross-Site Scripting (XSS). Larritasun handiko ahultasun horretarako CVE-2020-12512 identifikatzailea esleitu da.
- Sistema Eragilearen komando batean erabilitako elementu berezien neutralizazio desegokia (OS Command Injection). Larritasun handiko ahultasun horretarako CVE-2020-12513 identifikatzailea esleitu da.
- NULL punteroaren erreferentzia eza. Tarteko larritasuna duen ahultasun horretarako CVE-2020-12514 identifikatzailea

esleitu da.
- Mugetatik kanpoko irakurketa. Larritasun handiko ahultasun horretarako CVE-2018-20679 identifikatzailea esleitu da.
- Akatsak gakoen administrazioan. Tarteko larritasuna duen ahultasun horretarako CVE-2018-0732 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna.

Schneider Electric erakundearen produktuen ahultasunak

Argitalpen data: 2021/01/07

Garrantzia: Altua

Kaltetutako baliabideak:

Los siguientes productos Modicon:

- M340 CPUak:
  - 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, TSXP576634, bertsio guztiak.
- Premium komunikazio moduluak:
  - TSXETY4103, bertsio guztiak;
  - TSXETY5103, tbertsio guztiak.
- Ethernet COPRO integratua duten quantum prozesatzaileak:
  - 140CPU65xxxxx, bertsio guztiak.
- Quantum komunikazio moduluak:
  - 140NOE771x1, bertsio guztiak;
  - 140NOC78x00, bertsio guztiak;
  - 140NOC77101, bertsio guztiak.

Azalpena:

Fortinet's FortiGuard Labs erakundeko Kai Wang-ek ahultasun horien berri eman dio Schneider Electric erakundeari. Horren bidez, erasotzaile batek datuen ustelkeria burutu edota web zerbitzariaren erorketa eragin lezake.

Konponbidea:

Modicon PAC kontrolatzaileen eguneratze bat dago aurreikusita. Eskuragarri egon arte, fabrikatzaileak honakoa gomendatzen du:

- UnityPro / Ecostruxure Control Expert bidez FTP desgaitzea. Aukera hori desaktibatuta dago berez, aplikazio berri bat sortzen denean.
- Ecostruxure Control Expert programazio tresnaren bidez sarbide-kontrolaren zerrenda konfiguratzea.
- Sarearen segmentazioa konfiguratzea, eta 21/TCP porturako baimenik gabeko sarbide oro blokeatzeko suebaki bat ezartzea.

Schneider Electric etxearen Modicon Premium eta Modicon Quantum kontrolatzaileak beren bizitza erabilgarriaren amaierara heldu dira eta ez daude merkatuan eskuragarri dagoeneko. Horien ordez, ePAC Modicom M580 izeneko kontrolagailua dago.

Xehetasunak:

- Mugetatik kanpoko irakurketaren motako ahultasun batek segmentazio akatsa edota bufferraren gainezkatzea eragin lezake, kontrolagailuan bereziki diseinatutako artxibo bat igotzen denean, FTP bidez. Ahultasun horretarako, CVE-2020-7562 identifikatzailea esleitu da.
- Mugetatik kanpoko idazketaren motako ahultasun baten ondorioz, datuen ustelkeria, erorketa, edo kodearen exekuzioa gerta liteke, kontrolagailuan bereziki diseinatutako artxibo bat igotzen denean, FTP bidez. Ahultasun horretarako, CVE-2020-7563 identifikatzailea esleitu da.
- Bufferraren gainezkatze motako ahultasun baten ondorioz, idazketa sarbidea eta komandoen exekuzioa gerta litezke, kontrolagailuan bereziki diseinatutako artxibo bat igotzen denean, FTP bidez. Ahultasun horretarako, CVE-2020-7564 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Schneider Electric, Windows.

Hainbat ahultasun General Electric etxearen produktu batzuetan

Argitalpen data: 2021/01/07

Garrantzia: Kritikoa

Kaltetutako baliabideak:

RT430, RT431 & RT434, bertsio honen aurreko guztiak: 08A06.

Azalpena:

Thales UK erakundeko Tom Westenberg ikertzaileak ahultasun horien berri eman dio GE erakundeari. Horien bidez, urrutiko erasotzaile batek, egiaztatuta, kode arbitrarioa exekuta lezake sisteman, edo trafiko enkriptatua antzeman eta deszifratu.

Konponbidea:

- 08A06 firmware bertsiora edo osteko batera eguneratu.

Honako arintze neurriek ez dute bermatzen erabateko segurtasuna, baina kontuan hartu behar dira, kaltetutako produktua eguneratu arte:

- Segurtasun fisiko handiko eta sareko babesa erabili erasotzaile bat normalean Reason RT43X delakoak instalatzen diren sarera heltzeko.
- TCP/IP 80 eta 443 portuak blokeatzea, Reason RT43X produktuak dituen web interfazerako HTTP/HTTPS sarbidea blokeatzeko. TCP/IP portuaren blokeo hori Reason RT43X konektatuta dagoen Ethernet portuaren interfazera mugatu behar da (esaterako, sarbide kontrolerako zerrenda erabiliz -ACL-). Bestela, beste HTTP/HTTPS aplikazio batzuk egon daitezke kaltetuta.
- Kontrol gailu edota azpisistema guztiak sarean ahalik eta gutxien egotea, eta Internet bidez sartu ezin dela ziurtatzea.
- Ustekabeko trafikoa edota komunikazioa garaiz antzemateko segurtasun-jarduerak aztertzea.

Xehetasunak:

- Webgunean kodearen injekzio motako ahultasun bat egonik, urrutiko erasotzaile batek, egiaztatuta, kode arbitrarioa exekuta lezake sisteman. Ahultasun horretarako, CVE-2020-25197 identifikatzailea esleitu da.
- Gako kriptografiko kodeturako sarbidea duen erasotzaile batek, trafiko zifratua antzeman eta deszifratu lezake, HTTPS konexio baten bidez. Ahultasun horretarako, CVE-2020-25193 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Mugetatik kanpoko irakurketa Panasonic FPWIN Pro sisteman

Argitalpen data: 2021/01/07

Garrantzia: Altua

Kaltetutako baliabideak:

- FPWIN Pro, 7.5.0.0 bertsioa eta aurrekoak.

Azalpena:

Francis Provencher ikertzaileak, Trend Micro Zero Day Initiative ekimenaren baitan, CISAri jakinarazi dio mugetatik kanpoko irakurketaren motako ahultasun bat dagoela, larritasun handikoa.

Konponbidea:

7.5.1.0 bertsiora eguneratzea.

Xehetasunak:

Urrutiko erasotzaile batek kode arbitrarioa exekuta lezake, erabiltzaile batek bereziki diseinatutako proiektu-artxibo bat zabaldu ostean. Ahultasun horretarako, CVE-2020-16236 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna

Hainbat ahultasun Red Lion Crimson sisteman

Argitalpen data: 2021/01/07

Garrantzia: Altua

Kaltetutako baliabideak:

- Crimson 3.1, 3119.001 bertsioaren aurreko guztiak.

Azalpena:

Marco Balduzzi, Ryan Flores, Philippe Lin, Charles Perine eta Rainer Vosseler ikertzaileek, Trend Micro Zero Day Initiative ekimenaren baitan, ahultasun batzuen berri eman diote CISAri: larritasun handiko bat, puntero nuluaren erreferentziaren motakoa; eta tarteko larritasuneko bi, egiaztatzerik ezaren eta memoriaren ihesaren motakoak.

Konponbidea:

3119.001 bertsiora edo osteko batera eguneratzea.

Xehetasunak:

- Erasotzaile batek gailua berrabiarazi lezake, bereziki diseinatutako pakete bat bidaliz. Ahultasun horretarako, CVE-2020-27279 identifikatzailea esleitu da.
- Aldez aurretiko konfigurazioaren bidez, erasotzaile batek datu-basea irakurri edo aldatu lezake, baimenik behar izan gabe. Ahultasun horretarako, CVE-2020-27285 identifikatzailea esleitu da.
- Baliabideen liberazio desegokiaren bidez, erasotzaile batek memoria ihes arbitrarioak eragin litzake, bereziki diseinatutako mezuak bidaliz. Ahultasun horretarako, CVE-2020-27283 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun Delta Electronics-en DOPSoft produktuan

Argitalpen data: 2021/01/07

Garrantzia: Altua

Kaltetutako baliabideak:

- DOPSoft, versiones 4.0.8.21 y anteriores.

Azalpena:

Kimiyak, Trend Microren Zero Day ekimenaren baitan lanean, larritasun handiko bi ahultasunen berri eman dio CISAri. Horien bidez, erasotzaile batek kodearen exekuzio arbitrarioa exekuta lezake.

Konponbidea:

- 4.00.10.17 bertsiora edo osteko batera eguneratzea.
- DOPSoft v4.00.10.17 bertsioa erabiltzea proiektu zaharrak zabaltzeko (*.dpa), eta gero artxibo berri gisa irekitzea, artxibo zaharrak ezabatu ostean.
- Aplikazioaren interakzioa artxibo fidagarrietara mugatzea.

Xehetasunak:

Mugetatik kanpoko idazketaren edo puntero nuluaren erreferentziaren motako ahultasunen bidez, erasotzaile batek kode arbitrarioa exekuta lezake, proiektu-artxiboak prozesatzen diren bitartean. Ahultasun horietarako CVE-2020-27275 eta CVE-2020-27277 identifikatzaileak erreserbatu dira.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Zerbitzu ukapena Rockwell Automation markaren RSLinx Classic sisteman

Argitalpen data : 2021/01/08

Garrantzia: Altua

Kaltetutako baliabideak:

RSLinx Classic 2.57.00.14 CPR 9 SR 3.

Azalpena:

Ethernet/IP zerbitzariaren funtzionalitatean ahultasun bat argitaratu da. Horren bidez, erasotzaile batek zerbitzu ukapena eragin lezake.

Konponbidea:

Momentuz, ez da konponbiderik eman.

Xehetasunak:

Ethernet/IP zerbitzariaren funtzionalitatearen ahultasun baten bidez, erasotzaile batek zerbitzuaren ukapena eragin lezake, bereziki landutako eskaera bat bidaliz. Ahultasun horretarako, CVE-2020-13573 identifikatzailea esleitu da.

Etiketak: Ahultasuna

Ahultasuna Eaton etxearen EASYsoft sisteman

Argitalpen data: 2021/01/08

Garrantzia: Ertaina

Kaltetutako baliabideak:

EASYsoft, 7.20 bertsioa eta aurrekoak.

Azalpena:

Francis Provencher ikertzaileak, Trend Micro's Zero Day Initiative ekimenarekin batera, CISAri eman dio ahultasun horren berri. Horren bidez, tokiko erasotzaile batek programa bat aldatu edo ustekabean ixtea eragin lezake.

Konponbidea:

- Eaton konponbide bat bilatzen ari da, eta urtarrilaren amaierarako dago aurreikusita.
- Kaltetuei gomendatu die iturri guztiz fidagarri batetik sortutako .E70 artxiboak soilik erabiltzeko, eta, .E70 artxiboaren karga dela eta aplikazioak huts eginez gero, aplikazioa berrabiarazteko eta .E70 artxibo hori berriz ez kargatzeko.

Xehetasunak:

Kaltetutako produktuak aukera ematen du puntero bat artxibo baten objektutik irakurtzeko, eta horrek moten nahastea eragin lezake. Ahultasun horretarako, CVE-2020-6656 identifikatzailea esleitu da.

Mugetatik kanpoko irakurketaren bidez, erasotzaile batek programa bat aldatu edo blokeatu lezake. Ahultasun horretarako, CVE-2020-6655 identifikatzailea esleitu da.

Etiketak: Azpiegitura kritikoak, Ahultasuna

Kodearen exekuzio arbitrarioa Delta Electronics erakundearen CNCSoft-B sisteman

Argitalpen data: 2021/01/08

Garrantzia: Altua

Kaltetutako baliabideak:

CNCSoft-B, 1.0.0.2 bertsioa eta aurrekoak.

Azalpena:

Kimiyak, Trend Micro's Zero Day Initiative ekimenarekin batera, hainbat ahultasunen berri eman dio CISAri. Horien bidez, erasotzaile batek kode arbitrarioa exekuta lezake.

Konponbidea:

Bertsio honetara egunratzea: CNCSoft-B v1.0.0.3.

Xehetasunak:

Mugetatik kanpoko idazketak, mugetatik kanpoko irakurketak, null punteroaren erreferentziarik ezaren arazoak edo motaren nahaste arazo batek, proiektuaren artxiboak prozesatzen diren bitartean, erasotzaile bati aukera emango lioke kode arbitrarioa exekutatzeko. Ahultasun horietarako CVE-2020-27287, CVE-2020-27291, CVE-2020-27289 eta CVE-2020-27293 identifikatzaileak esleitu dira.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun Innokas Yhtymä Oy enpresaren Vital Signs Monitor VC150 sisteman

Argitalpen data: 2021/01/08

Garrantziaa: Tartekoa

Kaltetutako baliabideak:

- Monitor Vital Signs VC150, 1.7.15 bertsioaren aurrekoak.

Azalpena:

ERNW erakundeko Julian Suleder, Nils Emmerich, Birk Kauer eta Oliver Matula ikertzaileek tarteko larritasuneko bi ahultasunen berri eman dute, bata cross-site scripting motakoa (XSS) eta bestea kodearen injekzio motakoa.

Konponbidea:

- 1.7.15b edo osteko bertsiora eguneratzea.
- Gainera, fabrikatzaileak honakoa gomendatzen du:
  - Sarea segmentatzea, VLAN erabiliz, eta gailuak segurtasun-baliabideen bidez isolatzea.
  - Babes fisikoak ezartzea, gailuetara baimenik gabe sartzea eragozteko.
  - Ospitaleko langileen artean segurtasunaren kontzientzia zabaltzea.

Xehetasunak:

- Erasotzaile batek web edo HTML komandoen sekuentzia arbitrarioak injekta litzake, artxiboaren izenaren

parametroaren bidez, administrazio webgunearen interfazearen puntu batzuetan. Ahultasun horretarako, CVE-2020-27262 identifikatzailea esleitu da.
- Erasotzaile batek HL7 v2.x mezuen segmentuak injektatu litzake hainbat parametroren bidez, barra kodearen irakurgailu bat erabiliz. Ahultasun horretarako, CVE-2020-27260 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Baimen desegokia Hitachi ABB Power Grids markaren FOX615 sisteman

Argitalpen data: 2021/01/08

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- FOX61xR1, CESM1/CESM2 erabiliz, honen aurreko bertsio guztiak: cesne_r1h07_12.esw;
- FOX61xR2, CESM1/CESM2 erabiliz, honen aurreko bertsio guztiak: cesne_r2d14_03.esw.

Azalpena:

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

Konponbidea:

- FOX61xR1: cesne_r1h07_12.esw edo osteko bertsio batera eguneratzea;
- FOX61xR2: cesne_r2d14_03.esw edo osteko bertsio batera eguneratzea.

Xehetasunak:

Erasotzaile batek bereziki diseinatutako mezu bat bidal lezake, komunikazio bide bat irekitzeko, egiaztatu beharrik gabe, eta urrutitik kodea exekutatu ahal izango luke. Ahultasun horretarako, CVE-2018-10933 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna

Hainbat ahultasun Omron markako CX-One produktuan

Argitalpen data: 2021/01/08

Garrantzia: Altua

Kaltetutako baliabideak:

- CX-One, 4.60 bertsioa eta aurrekoak, honako aplikazioak barne:
  - CX-Protocol, 2.02 bertsioa eta aurrekoak;
  - CX-Server, 5.0.28 bertsioa eta aurrekoak;
  - CX-Position, 2.52 bertsioa eta aurrekoak.

Azalpena:

Rgod ikertzaileak, Trend Micro-ren Zero Day Initiative ekimenarekin lan eginez, ahultasun batzuen berri eman dio CISAri; larritasun handiko bat, bufferraren gainezkatze motakoa; eta tarteko larritasuneko bi, kodearen urrutiko exekuzioaren motakoak..

Konponbidea:

Eguneratzea:

- CX-Protocol 2.03 bertsioa;
- CX-Server 5.0.29 bertsioa;
- CX-Position 2.53 bertsioa.

Xehetasunak:

- Pilan oinarritutako bufferraren gainezkatze motako ahultasun baten ondorioz (stack), erasotzaile batek kodearen exekuzio arbitrarioa burutu lezake. Ahultasun horretarako, CVE-2020-27261 identifikatzailea esleitu da.
- Gainerako ahultasunetarako, identifikatzaile batzuk esleitu dira: CVE-2020-27259 eta CVE-27257.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna

Siemens segurtasun oharrak, 2021eko urtarrila

Argitalpen data: 2021/01/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SCALANCE X-200 (SIPLUS NET aldaerak barne), bertsio guztiak;
- SCALANCE X-200IRT (SIPLUS NET aldaerak barne), bertsio guztiak;
- SCALANCE X-300 (X408 eta SIPLUS NET aldaerak barne), V4.1.0 bertsioaren aurrekoak;
- JT2Go, V13.1.0 bertsioaren aurrekoak;
- Teamcenter Visualization, V13.1.0 bertsioa eta aurrekoak;
- Solid Edge, SE2021MP2ren aurreko bertsioak;

Azalpena:

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

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneratzeak Siemens deskarga paneletik deskargatu daitezke. Eguneratzerik gabeko produktuetarako, Erreferentzien atalean azaldutako arintze-neurriak aplikatu behar dira.

Xehetasunak:

Siemensek, segurtasun partxeei buruzko hileroko jakinarazpenean, 12 segurtasun-abisu eman ditu; horietatik 8 eguneratzeak dira.

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Mugaz kanpoko idazketaren 10 ahultasun,
- Pilan oinarritutako buffer gainezkatzearen 6 ahultasun (Stack),
- Memoria dinamikoan oinarritutako buffer gainezkatzearen arloko 5 ahultasun (Heap),
- Mota ez bateragarri bidezko baliabide-sarbidearen motako 2 ahultasun (mota nahasketa),
- Gako kriptografiko barneratuaren motako 2 ahultasun,
- Funtzio kritikoko egiaztatze-gabeziaren ahultasun bat,
- Puntero ez fidagarrirako erreferentziarik ezaren motako ahultasun bat,
- XML Kanpo erakunderako erreferentziaren mugatze desegokiaren motako ahultasun bat (XXE),
- Mugaz kanpoko irakurketaren ahultasun bat,

Ahultasun horietarako, honako identifikatzaileak erreserbatu dira:

CVE-2020-15799, CVE-2020-15800, CVE-2020-25226, CVE-2020-28391, CVE-2020-28395, CVE-2020-26980, CVE-2020-26981, CVE-2020-26982, CVE-2020-26983, CVE-2020-26984, CVE-2020-26985, CVE-2020-26986, CVE-2020-26987, CVE-2020-26988, CVE-2020-26989, CVE-2020-26990, CVE-2020-26991, CVE-2020-26992, CVE-2020-26993, CVE-2020-26994, CVE-2020-26995, CVE-2020-26996, CVE-2020-28383, CVE-2020-28381, CVE-2020-28382, CVE-2020-28383, CVE-2020-28384, CVE-2020-28386 eta CVE-2020-26989.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Siemens, Ahultasuna.

Schneider Electric erakundearen produktuen ahultasunak

Argitalpen data: 2021/01/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- EcoStruxure Power Build - Rapsody, 2.1.13 bertsioak eta aurrekoak;
- EcoStruxureTM Operator Terminal Expert 3.1 Service Pack 1A eta aurrekoak, Harmony HMIs-ekin:
  - HMIST6 serieak,
  - HMIG3U, HMIGTU serieak,
  - HMISTO serieak.
- Pro-face BLUE 3.1 Service Pack 1A eta aurrekoak, Pro-face HMIs-ekin:
  - ST6000 serieak,
  - SP-5B41 SP5000 serietan,
  - GP4100 serieak.

Azalpena:

Schneider Electric erakundeak bere produktu batzuei eragiten dieten larritasun handiko hiru ahultasunen berri eman du.

Konponbidea:

- EcoStruxure Power Build - Rapsody sistemaren ahultasunerako konponbidea 2021eko lehenengo hiruhilekorako dago aurreikusita, une horretara arte, fabrikatzaileak honakoa gomendatzen du:
  - Pribilegio txikienaren printzipioa aplikatzea, Rapsody softwarea exekutatzen duen konputagailurako sarbidea mugatzeko.
  - Aplikazioen zerrenda zuri bat ezartzea, kode maltzurraren exekuzioa blokeatzeko.
  - Ordenagailuan antibirus bat instalatzea eta eguneratuta mantentzea.
- Eguneraketa hau egitea: EcoStruxureTM Operator Terminal Expert V3.1 Service Pack 1B;
- Eguneraketa hau egitea: Pro-face BLUE V3.1 Service Pack 1B;

Xehetasunak:

- SSD artxibo maltzur bat igo eta modu desegokian aztertzen denean, erasotzaile batek aurretik liberatutako memoriaren erabileraren baldintza eragin lezake (use-after-free), edo pilan oinarritutako bufferraren gainezkatzea (stack), eta urrutiko kodea exekutatuko litzateke. Ahultasun horietarako CVE-2021-22697 eta CVE-2021-22698 identifikatzaileak erreserbatu dira.
- Sarbide desegokiaren balioztatze motako ahultasun baten bidez, erasotzaile batek kode arbitrarioa exekuta lezake, Ethernet Download funtzioa HMIan gaituta dagoenean. Ahultasun horretarako, CVE-2020-28221 identifikatzailea esleitu da.

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

Hainbat ahultasun SOOIL produktu batzuetan

Argitalpen data: 2021/01/13

Garrantzia: Altua

Kaltetutako baliabideak:

- Dana Diabecare RS, 3.0 bertsioaren aurreko guztiak;
- AnyDana-i, 3.0 bertsioaren aurreko guztiak;
- AnyDana-A, 3.0 bertsioaren aurreko guztiak.

Azalpena:

ERNW Research GmbH erakundeko Julian Suleder, Birk Kauer, Raphael Pavlidis eta Nils Emmerich ikertzaileek larritasun handiko ahultasun baten berri (gako deterministen motakoa) eta tarteko larritasuneko 8 ahultasunen berri eman diote Informazioaren Segurtasunerako Bulego Federalari (BSI).

Konponbidea:

- Eguneratzea:
  - Dana Diabecare RS 3.0 bertsiora, ostekoa edo eskuragarri dagoen azkena.
  - AnyDana-i eta AnyDana-A 3.0 bertsiora edo osteko batera.
- Gainera, fabrikatzaileak gomendatzen du Dana RS ezin eguneratzekotan, beti Airplane Mode sisteman erabiltzeko.

Xehetasunak:

Erasotzaile batek, fisikoki gertukoa eta baimenik gabe, indarrezko eraso bat burutu lezake Bluetooth Low Energy bidez, komunikazio protokoloak erabiltzen dituen gako determinista baliatuz. Ahultasun horretarako, CVE-2020-27264 identifikatzailea esleitu da.

Gainerako ahultasunetarako, identifikatzaile batzuk esleitu dira: identificadores CVE-2020-27256, CVE-2020-27258, CVE-2020-27266, CVE-2020-27268, CVE-2020-27269, CVE-2020-27270, CVE-2020-27272 eta CVE-2020-27276.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Osasuna, Ahultasuna.

Ahultasuna WAGO/M&M Software enpresaren fdtContainer sisteman

Argitalpen data: 2021/01/15

Garrantzia: Altua

Kaltetutako baliabideak:

- fdtCONTAINER component:
  - 3.5aren aurreko bertsioak;
  - 3.5.0 bertsioak, 3.5.20304.x-ren aurrekoak.
  - 3.6.0 bertsioak, 3.6.20304.x-ren aurrekoak.
- fdtCONTAINER application:
  - 4.5aren aurreko bertsioak;
  - 4.5.0 bertsioak, 4.5.20304.x-ren aurrekoak.
  - 4.6.0 bertsioak, 4.6.20304.x-ren aurrekoak.
- dtmINSPECTOR:
  - 3 bertsioa (FDT 1.2.x sisteman oinarritua).

Azalpena:

fdtCONTAINER component sistemaren bezero batek larritasun handiko ahultasun horren berri eman du, erakundeak koordinatuta. Horren bidez, erasotzaile batek kode maltzurra exekuta lezake.

Konponbidea:

Fabrikatzaileak bi konponbide posible proposatu ditu::

- Batetik, proiektuaren datuen deserializazio seguruagoa batera eguneratzea. Bertsio horiek teknologia zahartua erabiltzen jarraituko dute, baina egun ezaguna den eraso bektorea zuzenduko dute, eta bateragarriak izango dira proiektu artxiboekin, ez manipulatuak:
  - fdtCONTAINER component, 3.6.20304.x bertsioa edo ostekoa;
  - fdtCONTAINER application, 4.6.20304.x bertsioa edo ostekoa.

- Bestalde, serializazio teknologia eguneratuarekin proiektuaren datuen deserializazio segurua ematen duen bertsio batera eguneratzea. Horren ondorioz, dauden proiektu-artxibo ez manipulatuekiko bateragarritasun eza sortzen da:
    - fdtCONTAINER component, 3.7 bertsioa eta ostekoa;
    - fdtCONTAINER application, 4.7 bertsioa eta ostekoa.

Xehetasunak:

Datu ez fidagarrien deserializazio motako ahultasun baten ondorioz, erasotzaile batek kode maltzurra exekuta lezake, host-aren aplikazioa exekutatzen den lan-estaziotik, aplikazio horren erabiltzaile-baimenekin. Ahultasun horretarako, CVE-2020-12525 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Ahultasuna Dnsmasq zerbitzuan, Kontrol Industrialerako Sistemetan

Argitalpen data: 2021/01/20

Garrantzia: Altua

Kaltetutako baliabideak:

Dnsmasq DNS eta DHCP zerbitzaria, 2.8.2 bertsioa eta aurrekoak.

Kontrol Industrialerako Sistema batzuei Dnsmasq zerbitzuaren ahultasun batek eragin die. Kaltetutako produktuen zerrenda osoa ikusteko, kontsultatu erreferentzien atala.

Azalpena:

DNSSEC dnsmasq zerbitzuaren ezarpenean hainbat ahultasun antzeman dira. Horien bidez, urrutiko erasotzaile batek, egiaztatu beharrik gabe, cachéa pozoitu lezake, informazioa zabaldu, kode arbitrarioa exekutatu edota zerbitzuaren ukapena eragin (DoS) kaltetutako gailu batean. Ahultasunak multzokatu eta DNSpooq izena jarri zaie.

Konponbidea:

- Bertsio honetara eguneratzea: dnsmasq 2.83.
- Honako neurriak gomendatu dira:
-
    - 2. geruzako segurtasun-ezaugarriak ezartzea, hala nola DHCP snooping eta IP iturriaren babesa.
    - Dnsmasq konfiguratzea, beharrezkoa ez bada WAN interfazeak ez entzuteko.
    - --dns-forward-max=< kontsultak > aukerarekin bidal daitekeen gehieneko kontsulta kopurua murriztea. Berez, balioa 150ekoa da, baina murriztu liteke.
    - NSSEC balioztatze-aukera aldi baterako desgaitzea, eguneratu arte.
    - Upstream zerbitzarira konektatzeko DNS-over-HTTPS edo DNS-over-TLS erabiltzea.
- Fabrikatzaile bakoitzaren neurri propioak ezagutzeko, kontsultatu erreferentzien atala.

Xehetasunak:

- DNSSECen datuekin balioztatu aurretik RRSets antolaketa bat egitearen ondorioz, memoria dinamikoan oinarritutako bufferraren gainezkatze motako ahultasun bat (Heap) sortu liteke, eta, horren bidez, erasotzaile batek kode arbitrarioa exekuta lezake bereziki diseinatutako DNS erantzun bat bidaliz. Ahultasun horretarako, CVE-2020-25681 identifikatzailea esleitu da.
- DNSSECen datuekin balioztatu aurretik DNS paketeen izenak ateratzearen ondorioz, memoria dinamikoan oinarritutako bufferraren gainezkatze motako ahultasun bat (Heap) sortu liteke, eta, horren bidez, erasotzaile batek kode arbitrarioa exekuta lezake bereziki diseinatutako DNS erantzun bat bidaliz. Ahultasun horretarako, CVE-2020-25682 identifikatzailea esleitu da.
- Memoria dinamikoan oinarritutako bufferraren gainezkatze motako ahultasunen ondorioz (Heap), DNSSEC aktibatuta dagoenean, jasotako sarbideak balioztatu aurretik, erasotzaile batek zerbitzua ukatu lezake, DNS erantzun baliodunak bidaliz. Ahultasun horietarako CVE-2020-25683 eta CVE-2020-25687 identifikatzaileak esleitu dira.
- Birbidalitako kontsulta baten erantzunean datuen egiazkotasuna behar bezala balioztatzen ez bada Dnsmasq zerbitzua forward.c:reply_query() sisteman konprobatzen ari denean erantzunaren xedeko helbidea / portua egiteke dauden kontsultek erabiltzen duten, erasotzaile batek DNSren cachéa pozoitzeko eraso bat burutu lezake. Ahultasun horretarako, CVE-2020-25684 identifikatzailea esleitu da.
- Algoritmo kriptografiko apurtu edo ahul bat erabiltzearen ondorioz, erasotzaile batek hainbat domeinu ezberdin aurki litzake hash berarekin, ibilbidetik kanpo, Dnsmasq bidez onartzeko erantzun bat faltsutzeko saiakera kopurua nabarmen murriztuz, eta DNSren cachéa pozoitzeko eraso bat burutu. Ahultasun horretarako, CVE-2020-25685 identifikatzailea esleitu da.
- Datuen egiazkotasuna behar den moduan balioztatzen ez bada, kontsulta bat jasotzean Dnsmasq zerbitzuak ez badu konprobatzen izen horrekin beste eskaerarik pendiente dagoen beste eskaera bat birbidali aurretik, erasotzaile batek, sareko ibilbidetik kanpo, Dnsmasq zerbitzuaren bidez onartzeko erantzun bat faltsutzeko saiakera kopurua murriztu lezake, eta DNSren cachéa pozoitzeko eraso bat burutu. Ahultasun horretarako, CVE-2020-25686 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, DNS, Azpiegitura kritikoak, Siemens, Ahultasuna.

Hainbat ahultasun Reolink-en P2P produktu batzuetan

Argitalpen data: 2021/01/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Serie hauetako produktu guztiak:

- RLC-4XX;
- RLC-5XX;
- RLN-X10.

Azalpena:

Nozomi Networks-ek bi ahultasunen berri eman dio CISAri; bata larritasun kritikokoa, eta beste larritasun handikoa. Horien bidez, erasotzaile batek informazio konfidentziala eskura lezake, edo sare lokaletik kanpoko ekipoak konprometitu.

Konponbidea:

Gomendioa: Reolink gailuetan P2P funtzioa desaktibatzea eta beren firmwarea eguneratzea.

Xehetasunak:

- Sare lokalerako sarbidea duen erasotzaile batek zifratze gako finko bat lortu lezake, eta, horren bidez, sare horretatik kanpoko P2P Reolink kamerak konprometitu. Ahultasun horretarako, CVE-2020-25173 identifikatzailea esleitu da.
- Gailu lokalaren eta Reolink zerbitzarien arteko datu-transferentziarako dagoen P2P protokoloaren segurtasun-faltaren bidez, erasotzaile batek informazio konfidentziala eskura lezake. Ahultasun horretarako, CVE-2020-25169 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Lan berezien neutralizazio okerra Philipsen lan-estazioetan

Argitalpen data: 2021/01/20

Garrantzia: Ertaina

Kaltetutako baliabideak:

12NC identifikazioko lan-estazioak, hauei dagokienez:

- 4598 009 39471;
- 4598 009 39481;
- 4598 009 70861;
- 4598 009 98531;

Software hau exekutatzen dutenak:

- Interventional Workspot, 1.3.2, 1.4.0, 1.4.1, 1.4.3 eta 1.4.5 bertsioak;
- Coronary Tools, 1.0 bertsioa;
- Dynamic Coronary Roadmap, 1.0 bertsioa;
- Stentboost Live, 1.0 bertsioa;
- ViewForum, 6.3V1L10 bertsioa.

Azalpena:

Philipsek CISAri eman dio tarteko larritasuneko ahultasun baten berri. Horren bidez, erasotzaile batek, sare barruan, urrutitik itzali edo berrabiarazi lezake lan-estazioetako bat.

Konponbidea:

- Philipsk partxe bat argitaratu du ahultasun horri modu proaktiboan heltzeko, eta babes-jarduerak programatuko ditu kaltetutako bezeroekin, zuzenketak ezartzeko.
- Arintze-neurri moduan, fabrikatzaileak gomendatu du lan-estazioaren interfazerako IPMI pasahitza aldatzea.

Xehetasunak:

Sistema eragilearen komandoetan erabiltzen diren elementu berezien neutralizazio desegokiaren ondorioz, erasotzaile batek komando horiek alda litzake, beste osagai batera bidaliak izanik. Ahultasun horretarako, CVE-2020-27298 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Osasuna

Hainbat ahultasun Bosch Fire Monitoring System sisteman

Argitalpen data: 2021/01/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Bosch FSM-2500, 5.2 bertsioa eta aurrekoak;
- Bosch FSM-5000, 5.2 bertsioa eta aurrekoak.

Azalpena:

Produktuaren barne-probak egin bitartean, Bosch erakundeak 2 ahultasun antzeman zituen, larritasun kritiko eta ertainekoak. FSMren 5.2 bertsioari eta aurrekoei eragiten diete (Fire Monitoring System).

Konponbidea:

FSM bertsio hauetara eguneratzea: 5.6 edo ostekoak.

Xehetasunak:

- Datu-basean barneratutako kredentzialen erabileraren bidez, urrutiko erasotzaile batek, baimenik gabe, datu-baserako sarbide izan lezake, administrari pribilegioekin. Horrela, gordetako datuen konfidentzialtasun eta integritate osoa konprometituta gera liteke, eta datu-base propioaren eskuragarritasun handia eragin. Gainera, erasotzaileak azpiko sistema eragilean komando arbitrarioak exekuta litzake. Larritasun kritikoko ahultasunerako CVE-2020-6779 identifikatzailea esleitu da.
- Datu-basean kredentzial ez seguruak erabiltzearen ondorioz, urrutiko erasotzaile batek, administrari pribilegioekin, beste erabiltzaile batzuen kredentzialak eskuratu litzake eta beren pasahitzak testu lau moduan berreskuratu, hash MD5eko erasoen bidez. CVE-2020-6780 identifikatzailea esleitu da tarteko larritasuna duen ahultasunerako.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Zerbitzu ukapenaren inguruko ahultasun bat ABBren AC500 V2 sisteman

Argitalpen data: 2021/01/21

Garrantzia: Altua

Kaltetutako baliabideak:

Ethernet interfazea duten AC500 V2 produktu guztiak.

Azalpena:

ABBk jakinarazi du AC500 V2 sisteman ahultasun bat dagoela, eta, horren bidez, erasotzaile batek zerbitzu ukapena eragin lezakeela. Gailua blokeatu ostean (ERR LED gorriz keinuka), gailua berrabiarazteko eskatzen da.

Konponbidea:

ABB erakundeak 2.8.5 firmware bertsioa argitaratu du, eta PLC modelo hauetan ahultasun hori zuzentzen du:

- PM573-ETH
- PM583-ETH

Kaltetutako beste PLC modelo batzuetarako, ABBren gomendioa da sare ez fidagarri edo publikoen bidez erakusgai ez egotea, eta firmware berri baten argitalpenaren zain egotea.

Xehetasunak:

ABB erakundeak jakinarazi du ahultasun bat dagoela, eta, horren bidez, erasotzaile batek zerbitzuaren ukapena eragin lezakeela kaltetutako PLCetan, baimenik gabeko pakete manipulatu bat bidaliz, eta blokeatzearen ostean (ERR LED gorriz keinuka), berrabiaraztea eskatuz. Ahultasun horretarako, CVE-2020-24685 identifikatzailea esleitu da.

Etiketak: Komunikazioak, Azpiegitura kritikoak, SCADA, Ahultasuna.

Hainbat ahultasun Delta Electronics-en zenbait produktutan

Argitalpen data: 2021/01/22

Garrantzia: Altua

Kaltetutako baliabideak:

- ISPSoft, 3.12 bertsioa eta lehenagokoak;
- TPEditor, 1.98 eta lehenagoko bertsioak.

Azalpena:

Francis Provencher eta kimiya segurtasun ikertzaileak, Trend Micro-ko ZDIrekin lankidetzan, larritasun altuko 3 ahultasunen berri eman dute. Horiek baliatuz erasotzaile batek kodea exekuta lezake aplikazioaren pribilegioekin.

Konponbidea:

- ISPSoft 3.12.01 bertsiora eguneratzea;
- TPEditor 1.98.03 bertsiora eguneratzea.

Xehetasunak:

- Aldez aurretik askatutako memoriaren erabilpen (use after free) erako arazo bat aurkitu da proiektuko fitxategien prozesamenduan. Hori baliatuz erasotzaile batek bereziki diseinatutako proiektu fitxategi bat sor lezake kode arbitrarioaren exekuzio bat egiteko. Ahultasun horretarako CVE-2020-27280 identifikatzailea erabili da.
- Fidagarria ez den erakuslearen deserreferentzia erako arazo bat aurkitu da proiektuko fitxategien prozesamenduan. Hori baliatuz erasotzaile batek bereziki diseinatutako proiektu fitxategi bat sor lezake kode arbitrarioaren exekuzio bat egiteko. Ahultasun horretarako CVE-2020-27288 identifikatzailea erabili da.
- Kaltetutako produktua ahula da mugez kanpoko idazketako bi instantziaren aurrean, proiektuko fitxategien prozesamenduan. Hori baliatuz erasotzaile batek bereziki diseinatutako proiektu fitxategi bat sor lezake kode arbitrarioaren exekuzio bat egiteko. Ahultasun horretarako CVE-2020-27284 identifikatzailea erabili da.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Ahultasuna

Hainbat ahultasun Matrikon-en OPC UA Tunneller-en

Argitalpen data: 2021/01/22

Garrantzia: Kritikoa

Kaltetutako baliabideak:

OPC UA Tunneller, 6.3.0.8233 baino lehenagoko bertsio guztiak.

Azalpena:

Claroty-ko Uri Katz ikertzaileak hainbat ahultasun aurkitu ditu Honeywell-ena den Matrikon markaren OPC UA Tunneller-en. Ahultasun horiek baliatuz urruneko erasotzaile batek informazio konfidentzialera sarbidea lor lezake, urrunetik kode arbitrarioa exekutatu edo gailua blokeatu eta zerbitzuaren ukapen egoera eragin.

Konponbidea:

Honeywell-ek gomendatzen du Matrikon OPC UA Tunneller 6.3.0.8233 bertsiora eguneratzea.

Xehetasunak:

OPC UA Tunneller-en aurkitutako ahultasun garrantzitsuena baliatuz, kode arbitrarioa exekuta liteke urrunetik heap-en oinarritutako bufferraren gainezkatzearen bidez, memoriako balioak manipulatuz eta kode arbitrarioaren exekuzioa eraginez. Ahultasun kritiko honetarako CVE-2020-27297 identifikatzailea erabili da.

Aurkitutako beste ahultasun batzuen identifikatzaileak honakoak dira: CVE-2020-27299, CVE-2020-27274 eta CVE-2020-27295.

Etiketak: Eguneraketa, Azpiegitura kritikoak, SCADA, Ahultasuna

---

Hainbat ahultasun Fuji Electric produktuetan

Argitalpen data: 2021/01/27

Garrantzia: Altua

Kaltetutako baliabideak:

- Tellus Lite V-Simulator, v4.0.10.0 baino lehenagoko bertsioak;
- V-Server Lite, v4.0.10.0 baino lehenagoko bertsioak.

Azalpena:

Fuji Electric-en produktu batzuek dituzten hainbat ahultasun argitaratu dira. Horiek baliatuz erasotzaile batek kodea exekuta lezake aplikazioaren pribilegio berdinekin.

Konponbidea:

v4.0.10.0 bertsiora eguneratzea:

- v4.0.10.0 Disk 1;
- v4.0.10.0 Disk 2.

Xehetasunak:

Aplikazioak proiektuaren fitxategiak prozesatzeko duen modua baliatuz, erasotzaile batek bereziki diseinatutako proiektu fitxategi bat sor lezake kode arbitrarioa exekutatzeko, ondoko ahultasunetako bat erabiliz:

- Pilan (stack) oinarritutako bufferraren gainezkatzea. Ahultasun horretarako CVE-2021-22637 identifikatzailea erabili da.

- Mugez kanpoko irakurketa. Ahultasun horretarako CVE-2021-22655 identifikatzailea erabili da.
- Mugez kanpoko idazketa. Ahultasun horretarako CVE-2021-22653 identifikatzailea erabili da.
- Hasieratu gabeko erakuslea. Ahultasun horretarako CVE-2021-22639 identifikatzailea erabili da.
- Memoria dinamikoan (heap) oinarritutako bufferraren gainezkatzea. Ahultasun horretarako CVE-2021-22641 identifikatzailea erabili da.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Ahultasuna

Autentifikazio desegokia 4CCT-n

Argitalpen data: 2021/01/28

Garrantzia: Altua

Kaltetutako baliabideak:

4CCT-EA6-334126BF, firmwarearen 3.23.77.8.33251 bertsioa.

Azalpena:

INCIBEk ZIV 4CCT gailuak duen ahultasun bati buruzko argitalpena koordinatu du, INCIBE-2021-0040 barne kodearekin, Aarón Flecha Menéndezek aurkitua.

Ahultasun horri CVE-2021-25910 kodea esleitu zaio. CVSS v3-ren arabera 7,6eko oinarrizko puntuazioa kalkulatu da, CVSSren kalkulua honakoa izanik: AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C/CR:H/IR:H/AR:M/MAV:A/MAC:L/MPR:X/MUI:R/MS:U/MC:H/MI:H/MA:H.

Konponbidea:

3.23.80.58.46120 bertsiora eguneratzea.

Era berean egoera hau konpon daiteke HTTPS sarbidea behartuz edo gailuetarako sarbide fisiko lokalak murriztuz.

Xehetasunak:

ZIV Automation-en 4CCT gailuan cookie parametroaren erabilpen desegoki bat baliatuz, erasotzaile batek aldaketak egin litzake kaltetutako gailuaren hainbat parametrotan erabiltzaile autentifikatu baten modura.

Ahultasunaren arrazoia da cookie parametroaren erabilpen okerra, ez baitauzka saioaren bahiketa ekiditeko beharrezkoak diren segurtasun mekanismo guztiak.

Ahultasuna baliatzeko erasotzaileak egon behar du kaltetutako gailua kokatuta dagoen sarearen barnean.

CWE-287: Autentifikazio okerra.

Denborazko lerrroa:
2020/07/04 - Ikertzaileen aurkikuntza.

2020/08/17 - Ikertzaileak harremanetan jarri ziren INCIBErekin.

2020/10/30 - Fabrikatzaileak ahultasuna konfirmatu zion INCIBEri.

2020/12/21 - ZIV-ek konfirmatu zuen fix bertsioa eta software bertsio berria argitaratuak izan zirela (Security Patch/new version).

20201/01/28 - INCIBEk ohartarazpena argitaratu zuen.

Ohartarazpen honi buruzko informazio gehiago baldin badaukazu, jarri INCIBErekin harremanetan, CNAri ahultasunen jakinarazpena webgunean adierazten den moduan.

Etiketak: 0day, Eguneraketa, CNA, Ahultasuna

Zerbitzuaren ukapena 4CCT-n

Argitalpen data: 2021

Garrantzia: Altua

Kaltetutako baliabideak:

4CCT-EA6-334126BF, firmwarearen 3.23.80.27.36371 bertsioa.

Azalpena:

IINCIBEk ZIV 4CCT gailuak duen ahultasun bati buruzko argitalpena koordinatu du, INCIBE-2021-0039 barne kodearekin, Aarón Flecha Menéndezek aurkitua.

Ahultasun horri CVE-2021-25909 kodea esleitu zaio. CVSS v3-ren arabera 8,2eko oinarrizko puntuazioa kalkulatu da, CVSSren kalkulua honakoa izanik: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:H/RL:O/RC:C/CR:X/IR:X/AR:M/MAV:N/MAC:X/MPR:X/MUI:N/MS:C/MC:N/MI:N/MA:H.

Konponbidea:

3.23.80.58.46120 bertsiora eguneratzea.

Era berean egoera hau konpon daiteke gailua instalatuz banda zabalera mugatua duen eta sarbiderako pribilegioak eskatzen dituen sare batean.

Xehetasunak:

ZIV Automation-en 4CCT gailua ahula da 7919 atakaren bitartez egiten diren zerbitzuaren ukapen erako erasoen aurrean.

Ahultasun hau baliatuz gero urruneko erasotzaile batek gailuaren funtzionamendua eten lezake, 7919 atakara bidalitako pakete berezien bidez.

Erasoa bukatu ondoren, gailuak pixkanaka berreskuratu egiten du bere funtzionamendu normala.

CWE-400: Baliabideen kontrolatu gabeko kontsumoa (baliabideen agortzea).

Denborazko lerroa:

2020/03/10 - Ikertzaileen aurkikuntza.

2020/05/25 - Ikertzaileak harremanetan jarri ziren INCIBErekin.

2020/07/03 - Fabrikatzaileak ahultasuna konfirmatu zion INCIBEri.

2020/12/21 - ZIV-ek konfirmatu zuen fix bertsioa eta software bertsio berria argitaratuak izan zirela (Security Patch/new version).

2021/01/28 - INCIBEk ohartarazpena argitaratu zuen.

Ohartarazpen honi buruzko informazio gehiago baldin badaukazu, jarri INCIBErekin harremanetan, CNAri ahultasunen jakinarazpena webgunean adierazten den moduan.

Etiketak: 0day, Eguneraketa, CNA, Ahultasuna

Ahultasuna Siemens-en SIMATIC HMI paneletan

Argitalpen data: 2021/01/29

Garrantzia: Altua

Kaltetutako baliabideak:

- SIMATIC HMI Comfort Panels (SIPLUS aldaerak barne), V16 Update 3a baino lehenagoko bertsio guztiak;
- SIMATIC HMI KTP Mobile Panels, V16 Update 3a baino lehenagoko bertsio guztiak.

Azalpena:

SIMATIC HMI panelek ahultasun bat daukate, eta hori baliatuz urruneko erasotzaile batek sarbide osoa lor lezake gailura, telnet zerbitzua gaituta badago.

Konponbidea:

Honako bertsioetara eguneratzea:

- SIMATIC HMI Comfort Panels V16 Update 3a edo goragokoa;
- SIMATIC HMI KTP Mobile Panels V16 Update 3a edo goragokoa.

Arriskua murriztearren, Siemensek gomendatzen du telnet desgaitzea HMI paneletan, gaituta badago (modu lehenetsian desgaituta).

Xehetasunak:

Telnet zerbitzua gaituta duten kaltetutako gailuek ez dute inolako autentifikaziorik behar zerbitzu honetarako. Hortaz, urruneko erasotzaile batek sarbide osoa lor lezake gailuan. Ahultasun horretarako CVE-2020-15798 identifikatzailea erabili da.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Siemens, Ahultasuna