2020ko Abuztuaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Hainbat ahultasun daude Delta Electronics etxearen Automation CNCSoft ScreenEditor sisteman

Argitalpen data: 2020/08/05

Garrantzia: Altua

Kaltetutako baliabideak:

Industrial Automation CNCSoft ScreenEditor, 1.01.23 bertsioa eta aurrekoak.

Azalpena:

Industrial Automation CNCSoft ScreenEditor sisteman hainbat ahultasun atzeman dira. Horien bidez, erasotzaile batek informazioa irakurri edo aldatu lezake, kode arbitrarioa exekutatu edo sistema ustekabean itxi.

Konponbidea:

CNCSoft ScreenEditor 1.01.26 bertsiora eguneratzea.

Xehetasunak:

- Pilan oinarritutako bufferrak gainezka egitearen motako ahultasunen ondorioz, erasotzaile batek informazioa irakurri edo aldatu lezake, kode arbitrarioa exekutatu edo sistema ustekabean itxi, bereziki diseinatutako proiektu-artxiboak prozesatuz. Ahultasun horretarako, CVE-2020-16199 identifikatzailea esleitu da.
- Mugetatik kanpoko hainbat irakurketa-ahultasunen ondorioz, erasotzaile batek informazioa irakurri edota aplikazioa blokeatu lezake, bereziki diseinatutako proiektu-artxiboen prozesamenduaren bidez. Ahultasun horretarako, CVE-2020-16201 identifikatzailea esleitu da.
- Hasi gabeko puntero bat bereziki diseinatutako artxiboen prozesatzearen bidez ustiatu daiteke. Horren ondorioz, erasotzaile batek informazioa irakurri edo aldatu lezake, kode arbitrarioa exekutatu, edo sistema ustekabean ixtea eragin. Ahultasun horretarako, CVE-2020-16203 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Neutralizazio desegokiaren ahultasuna Geutebrück etxearen G-Cam eta G-Code sistemetan

Argitalpen data: 2020/08/07

Garrantzia: Altua

Kaltetutako baliabideak:

- 1.12.0.25 firmware bertsioa eta aurrekoak;
- Encoder eta E2 Series Camera eredu hauen 1.12.13.2 eta 1.12.14.5 bertsioak:
-
    - G-Code:
        - EEC-2xxx,
    - G-Cam:

- EBC-21xx,
- EFD-22xx,
- ETHC-22xx,
- EWPC-22xx.

Azalpena:

RandoriSec enpresako Davy Douhine ikertzaileak ahultasun horren berri eman dio CISAri. Larritasun handikoa da, eta, horren bidez, erasotzaile batek komandoak exekuta litzake root erabiltzaile gisa.

Konponbidea:

1.12.0.27 firmware bertsiora eguneratzea.

Xehetasunak:

Sistema eragilearen komandoetan erabilitako elementu berezien neutralizazioak aukera eman liezaioke erasotzaile bati root erabiltzaile gisa komandoak exekutatzeko, bereziki diseinatutako URL komando gisa. Ahultasun horretarako, CVE-2020-16205 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna

Hainbat ahultasun Advantech etxearen HMI Designer sisteman

Argitalpen data: 2020/08/07

Garrantzia: Kritikoa

Kaltetutako baliabideak:

WebAccess HMI Designer, 2.1.9.31 bertsioa eta aurrekoak.

Azalpena:

Kimiya eta Natnael Samson ikertzaileek, Trend Micro-ren Zero Day Initiative egitasmoarekin elkarlanean, 6 ahultasunen berri eman diote CISAri; bat larritasun kritikokoa da, 4 altukoak, eta beste bat baxukoa. Motak: pilan oinarritutako buffer gainezkatzea, heap motako buffer gainezkatzea, mugetatik kanpoko irakurketa, mugetatik kanpoko idazketa, mota ez bateragarriko baliabiderako sarbidea eta free funtziorako dei bikoitza.

Konponbidea:

Advantech etxeak WebAccess HMI Designer 2.1.9.81 bertsioa argitaratu du, ahultasun horiek konpontzeko.

Xehetasunak:

- Erabiltzaileak emandako datuen balioztatze egokirik gabeko bereziki diseinatutako proiektu-artxiboak prozesatuz gero, pilan oinarritutako (stack) buffer gainezkatzea gerta liteke; horren ondorioz, kodearen urrutiko exekuzioa gertatuko litzateke, informazioaren zabalkunde edo aldaketa, edota aplikazioaren blokeoa. Ahultasun horretarako, CVE-2020-16215 identifikatzailea esleitu da.
- Heap motako buffer gainezkatze ahultasunak ustiatu litezke bereziki diseinatutako proiektu-artxiboak irekiz, kodearen urrutiko exekuzioa burutzeko, informazioa zabaldu edota aldatu, edo aplikazioa blokeatzeko. Ahultasun horretarako, CVE-2020-16207 identifikatzailea esleitu da.
- Erabiltzaileak emandako datuen balioztatze egokirik gabeko bereziki diseinatutako proiektu-artxiboak prozesatuz gero, aurreikusitako buffer eremutik kanpo idatz lezake sistemak; horren ondorioz, kodearen urrutiko exekuzioa gertatuko litzateke, informazioaren zabalkunde edo aldaketa, edota aplikazioaren blokeoa. Ahultasun horretarako, CVE-2020-16213 identifikatzailea esleitu da.
- Erabiltzaileak emandako datuen balioztatze egokirik gabeko bereziki diseinatutako proiektu-artxiboak prozesatuz gero, moten nahasketa gerta liteke; horren ondorioz, kodearen urrutiko exekuzioa gertatuko litzateke, informazioaren zabalkunde edo aldaketa, edota aplikazioaren blokeoa. Ahultasun horretarako, CVE-2020-16229 identifikatzailea esleitu da.
- Bereziki diseinatutako proiektu-artxiboen prozesatzeak eragindako memoria askatzeko funtzioaren ahultasunaren ondorioz, kodearen urrutiko exekuzioa burutu liteke, informazioa zabaldu edota aldatu, edo aplikazioa blokeatu. Ahultasun horretarako, CVE-2020-16217 identifikatzailea esleitu da.
- Mugetatik kanpoko irakurketaren ahultasun bat baliatu liteke, bereziki diseinatutako proiektu-artxiboak prozesatzean, erasotzaile batek informazio hori irakurri ahal izateko. Ahultasun horretarako, CVE-2020-16211 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura Kritikoak, Ahultasuna

Hainbat ahultasun Delta Industrial Automation TPEditor sisteman

Argitalpen data: 2020/08/07

Garrantzia: Altua

Kaltetutako baliabideak:

TPEditor, 1.97 bertsioa eta aurrekoak.

Azalpena:

Delta testuaren programazio softwarean hainbat ahultasun atzeman dira. Horien bidez, erasotzaile batek informazioa irakurri edo aldatu lezake, kode arbitrarioa exekutatu edo sistema ustekabean itxi.

Konponbidea:

Delta Industrial Automation TPEditor eguneratzea, 1.98 bertsioa.

Xehetasunak:

Hainbat ahultasun, mugetatik kanpoko irakurketa motakoak, pilan oinarritutako bufferrak gainezka egitea, heap motako bufferraren gainezkatzea, sarrera datuen balioztatze okerra eta write-what-where baldintza. Ahultasun horien ondorioz, erasotzaile batek informazioa irakurri edo aldatu lezake, kode arbitrarioa exekutatu edo sistema ustekabean itxi, bereziki diseinatutako proiektu-artxiboak prozesatuz. Ahultasun horietarako CVE-2020-16299, CVE-2020-16221, CVE-2020-16227 eta CVE-2020-16225 identifikatzaileak esleitu dira.

Etiketak: Eguneratzea, Ahultasuna, Azpiegitura kritikoak.

Informazio sentikorra erremolkeetarako PLC sistemetan

Argitalpen data: 2020/08/07

Garrantzia: Ertaina

Kaltetutako baliabideak:

Erremolkeen linea elektrikoaren bidezko komunikazio guztiak kaltetuta daude.

Azalpena:

National Motor Freight Traffic Association (NMFTA) eta Assured Information Security (AIS) erakundeetako ikertzaileek ahultasun bat atzeman dute, informazio sentikorra zabaltzen dutenetakoa, hainbat fabrikatzaileren erremolkeetan erabilitako PLC sistemetan.

Konponbidea:

Ez da ahultasuna arintzeko sistemarik garatu, baina Cybersecurity and Infrastructure Security Agency (CISA) erakundeak gomendatu du neurri batzuk ebaluatzeko, hala nola PLC bus laburragoak erabiltzea erremolkeetan PLC bidez transmititutako informazioa agerian geratzeko arriskua murrizteko.

Xehetasunak:

Ikertzaileek deskubritu dute ECU (Engine Control Unit, motor kontrolaren unitatea) sistemara informazioa bidaltzeko erabiltzen diren PLC bidezko komunikazioak metro eta erdi eta bi metro bitarteko distantziara atzeman daitezkeela; baina, hargailu hobeekin, distantzia handiagoa ere izan daitekeela uste da.

Kasu gehienetan, informazio hori ABS sistema eta balazta sistemen egoera komunikatzeko erabiltzen da, baina, ahultasunaren berri zabalduz, bestelako informazio konfidentziala transmititzea ere saihestu nahi da, sistema hori atzemateko arriskua dela eta.

Ahultasun horretarako, CVE-2020-14514 identifikatzailea erreserbatu da.

Etiketak: Komunikazioak, Azpiegitura kritikoak, IoT, Pribatutasuna, Ahultasuna.

Siemensen segurtasun buletina. 2020ko abuztua

Argitalpen data: 2020/08/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SICAM A8000 RTUs-erako SICAM WEB firmwarea, V05.30 bertsioaren aurreko guztiak;
- Automation License Manager 5, bertsio guztiak;
- Automation License Manager 6, V6.0.8 bertsioaren aurreko guztiak;
- SIMATIC RF350M, bertsio guztiak;
- SIMATIC RF650M, bertsio guztiak;
- SIMOTICS CONNECT 400, bertsio guztiak;
- Desigo CC, 3.X eta 4.X bertsioak;
- Desigo CC Compact, 3.X eta 4.X bertsioak;
- RUGGEDCOM RM1224, V6.3 bertsioaren aurreko guztiak;
- SCALANCE M-800 / S615, V6.3 bertsioaren aurreko guztiak;

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, 20 segurtasun-abisu eman ditu; horietatik 15 eguneratzeak dira.

Argitaratutako ahultasun mota honakoei dagokie:

- Web orria sortu bitarteko sarreraren neutralizazio desegokiaren arloko ahultasun bat (Cross-site Scripting);
- Eguneratze desegokiaren arloko ahultasun bat;
- TOCTOU (Time-of-check Time-of-use) karrera izaerako ahultasun bat;
- Kodea sortzearen inguruko kontrol desegokiaren arloko ahultasun bat (kodea injektatzea);
- Sarrera tamainaren konprobaziorik gabeko bufferraren ahultasun bat (bufferrak gainezka egite klasikoa).

Ahultasun horietarako, honako identifikatzaileak erreserbatu dira: CVE-2020-15781, CVE-2020-7583, CVE-2019-15126, CVE-2020-10055 eta CVE-2020-8597.

Etiketak: Eguneraketa, Siemens, Ahultasna

Schneider erakundearen produktuen ahultasunak

Argitalpen data: 2020/08/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SoMove V2.8.1 eta aurrekoak;
- Harmony® eXLhoist base stations v04.00.02.00 eta aurrekoak:
  - ZARB12W;
  - ZARB12H;
  - ZARB18H;
  - ZARB18W;
  - ZARB18HM;
  - ZARB18WM.
- PowerChute Business Edition software V9.0.x eta aurrekoak;
- Modicon M218 Logic Controller V5.0.0.7 eta aurrekoak;
- Honako hardware bertsio guztiak:
  - spaceLYnk;
  - Wiser for KNX (homeLYnk).
- Schneider Electric Modbus Serial Driver (64 bits) V3.20 IE 30 bertsioaren aurrekoak;
- Schneider Electric Modbus Serial Driver (32 bits) V2.20 IE 30 bertsioaren aurrekoak;
- Schneider Electric Modbus Driver Suite, V14.15.0.0 bertsioaren aurrekoak, honako produktuetan erabiliz:
  - Ecostruxure Control Expert (Unity Pro gisa formalki ezaguna);
  - Unity Loader;
  - EcoStruxure Process Expert (Hybrid DCS gisa formalki ezaguna);
  - EcoStruxure OPC UA Server Expert;
  - OPC Factory Server;
  - Advantys Configuration Software;
  - Modbus Communications DTM (Field Devices);
  - SoMove;
  - Ecostruxure Machine Expert (SoMachine gisa formalki ezaguna);
  - Ecostruxure Machine Expert Basic;
  - Harmony® eXLhoist;
  - EcoStruxure Power Commission.
- SFAPV9601 - APC Easy UPS On-Line Software V2.0 eta aurrekoak.

Azalpena:

Schneider etxeak 8 argitalpenen berri eman du; horietako hiruk tarteko larritasuna dute, eta beste bi larritasun kritikokoak dira. Horien ondorioz, erasotzaile batek pribilegioetan gora egin lezake, zerbitzuaren ukapena burutu, kodearen urrutiko exekuzioa egin, sistema blokeatu, indarrez pasahitza baliatu edota exekuta daitezkeen fitxategiak igo.

Konponbidea:

Eguneratzea:

- SoMove V2.8.2;
- Harmony® eXLhoist base stations V04.00.03.00;
- PowerChute Business Edition software 9.1;
- Modicon M218 Logic Controller Firmware V5.0.0.8;
- SpaceLYnk v2.5.1;
- Wiser for KNX (homeLYnk) v2.5.1;
- Schneider Electric Modbus Serial Driver Suite V14.15.0.0;
- SFAPV9601 - APC Easy UPS On-Line Software V2.1.

Xehetasunak:

Larritasun kritikoko ahultasunak direktorio mugatu baterako ibilbide-izenaren luzera desegokiaren motakoak dira (Path Traversal), eta, horien ondorioz, erasotzaileak fitxategi exekutagarriak karga ditzake direktorio ez zehaztuetan, "FileUploadServlet" edo "SoundUploadServlet" metodo ahulen bidez. Ahultasun horietarako CVE-2020-7521 eta CVE-2020-7522 identifikatzaileak erreserbatu dira.

Kritikotasun ertain edo baxuko gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2020-7527, CVE-2019-19193, CVE-2020-7524, CVE-2020-7526, CVE-2020-7525 eta CVE-2020-7523.

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

Ahultasun bat atzeman da Tridium etxearen Niagara sisteman

Argitalpen data: 2020/08/12

Garrantzia: Ertaina

Kaltetutako baliabideak:

- Niagara: 4.6.96.28, 4.7.109.20, 4.7.110.32 eta 4.8.0.110 bertsioak,
- Niagara Enterprise Security: 2.4.31, 2.4.45 eta 4.8.0.35 bertsioak.

Azalpena:

Tridium etxeak jakinarazi du Niagara ekipoetan ahultasun bat dagoela. Horren bidez, erasotzaile batek baliabideak agortzea eragin lezake.

Konponbidea:

Tridium etxeak honako eguneratzeak argitaratu ditu:

- Niágara: 4.9.0.198,
- Niagara Enterprise Security: 4.9.0.60.

Eguneratzeak eskuragarri daude Tridium taldearen laguntza-kanalean.

Xehetasunak:

Atzemandako ahultasunaren jatorria honakoa da: TLS lotura protokolo baten denbora agortzea, konexioa bukaraziz. Horren ondorioz, Niagara eskegita geratzen da eta eskuz berrabiarazi beharra dago.

Ahultasun horretarako, CVE-2020-14483 identifikatzailea erreserbatu da.

Etiketak: IoT, SSL/TLS , Ahultasuna

Zerbitzu ukapena B&R etxearen Automation Runtime sisteman

Argitalpen data: 2020/08/13

Garrantzia: Ertaina

Kaltetutako baliabideak:

Automation Runtime bertsioak: 4.1x, 4.2x, 4.3x, 4.4x, 4.5x, 4.6x, 4.7x bertsioen aurrekoak.

Azalpena:

R&B etxeak Automation Runtime sistemaren ahultasun baten berri eman du. TFTP zerbitzuari eragiten dio eta erasotzaile batek zerbitzuaren ukapena eragin lezake produktuan.

Konponbidea:

Ahultasun hori konpontzeko, honako partxeak egokitu dira:

- 4.1x bertsioaren aurrekoak; R&B etxeak goragoko bertsio batera eguneratzea gomendatzen du,
- 4.2x: N4 26,
- 4.3x: N4 34,
- 4.4x: F4 45,
- 4.5x: E4 53,
- 4.6x: D4 63 (Q4 2020 bertsiorako planeatutako argitalpena),
- 4.7x: A4 73.

Xehetasunak:

Automation Runtime gailuen erabiltzen duten sistema eragilean TFTP zerbitzua ezartzeak arazo bat dauka memoriaren kudeaketan; izan ere, aurretik esleitutako memoria ez du askatzen, eta erasotzaile batek bereziki diseinatutako eskaerak bidal litzake TFTP zerbitzura, gailuaren memoria agortzeko asmoz.

Ahultasun horretarako, CVE-2020-11637 identifikatzailea erreserbatu da.

Etiketak: SCADA, Ahultasuna

Hainbat ahultasun Philips SureSigns VS4 sisteman

Argitalpen data: 2020/08/20

Garrantzia: Ertaina

Kaltetutako baliabideak:

Pazienteen monitorizaziorako Philips SureSigns VS4 sistema, A.07.107 bertsioa eta aurrekoak.

Azalpena:

Philipsek 3 ahultasunen berri eman du, bere jakinarazpen politikaren arabera. Horietako 2 tarteko larritasunekoak dira, eta bat baxukoa. Motak: sarbide desegokiaren balioztatzea, zifratze-indar desegokia eta sarbide-kontrol desegokia.

Konponbidea:

Philipsek gomendatzen du bezeroek sistemaren pasahitz guztiak aldatzea beren gailuetan. Bakoitzerako pasahitz bakarrak jartzea eta erabiltzen ari ez direnean fisikoki segurtatzea. Gomendatzen da, baita ere, bezerok pentsatzea ea Philips SureSigns VS4 gailuak beste teknologia berriago batengatik ordeztu nahi dituzten.

Xehetasuna:

Arrakastaz baliatuta, baimendu gabeko erabiltzaile batek administrazio kontrolak lortu litzake, eta sistemaren konfigurazioa, pazientearen datuak urrutiko leku batera bidalaraziz. Ahultasun honek ez dio pazientearen segurtasunari eragiten.

Etiketak: Azpiegitura kritikoak, Osasuna, Ahultasuna.

Hainbat ahultasun Moxaren NPort IAW5000A-I/O Series sisteman

Argitalpen data: 2020/08/20

Garrantzia: Handia

Kaltetutako baliabideak:

NPort IAW5000A-I/O Series, *firmware* 2.1 bertsioak edo aurrekoak.

Azalpena:

Evgeniy Druzhinin eta Ilya Karpov, Rostelecom-Solar ikertzaileek hainbat ahultasunen berri eman diote Moxari. Motak: saioa finkatzea, pribilegioen kudeaketa desegokia, pasahitz ahulen baldintzak, informazio konfidentziala daukan zifratu gabeko testuaren transmisioa, gehiegizko baimen-eskaeren mugatze desegokia eta informazioa zabaltzea.

Konponbidea:

Produktuaren *firmwarea* eguneratzea 2.2. bertsioaren arabera.

Xehetasuna:

Ahultasun horiek arrakastaz baliatuz gero, erasotzaile batek saioa bahitu lezake erabiltzailearen cookieak lapurtuz, administrari pribilegioekin eskaerak egin, kredentzial ahulak erabili, web zerbitzariak hirugarrenen zerbitzuen kredentzialak transmititu formaturik gabe, indarreko erasoak erabili SSH/Telnet saio batean baimena ematea saihesteko, eta web zerbitzu integratuan informazio konfidentziala lortu dagokion baimenik gabe.

Etiketak: Eguneratzea, Komunikazioak, IoT, Ahultasuna

Direktorio mugatu baterako mugatze ez zuzena Advantech iView sisteman

Argitalpen data: 2020/08/26

Garrantzia: Kritikoa

Kaltetutako baliabideak:

iView, 5.7 bertsioa eta aurrekoak.

Azalpena:

Trend Microren Zero Day Iinitiative ekimeneko KPCk CISAri eman zion ahultasun horren berri. Larritasun kritikokoa da, direktorio mugatu baterako ibilbide-izenaren mugatze okerrekoa (*path traversal*).

Konponbidea:

iView bertsio honetara ezagutzea: 5.7.02.

Xehetasuna:

Kaltetutako produktua mugatutako direktorio baterako ibilbide baten izenaren mugatze okerraren mende dago (*path traversal)*. Horren bidez, erasotzaile batek artxibo arbitrarioak sortu edo deskargatu litzake, sistemaren eskuragarritasuna mugatu eta kodea urrutitik exekutatu. Ahultasun horretarako, CVE-2020-16245 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Bufferrak gainezka egitea WECON etxearen LeviStudioU sisteman

Argitalpen data: 2020/08/26

Garrantzia: Handia

Kaltetutako baliabideak:

LeviStudioU, 2019-09-21 bertsioa eta aurrekoak.

Azalpena:

Natnael Samsonek, Trend Micro erakundearen Zero Day Initiative ekimenarekin batera, ahultasun horren berri eman zion CISAri, larritasun handikoa, pilan oinarritutako buffer gainezkatze motakoa (*stack).*

Konponbidea:

WECON erakundeak badaki arazoa zein den, eta konponbide bat garatzen ari da. Informazio gehiago lortzeko, WECON online zerbitzuarekin kontakta daiteke, edo telefonoz: 0086-591-87868869-894.

Xehetasuna:

Bereziki diseinatutako proiektu-artxibo bat irekitzeko ekintzaren bidez, erasotzaile batek bufferraren gainezkatze motako ahultasuna baliatu lezake eta aplikazioaren pribilegioen arabera kodea exekutatu. Ahultasun horretarako, CVE-2019-16243 identifikatzailea erreserbatu da.

Etiketak: Azpiegitura kritikoak, Ahultasuna

Zifratze akatsak Emersonen OpenEnterprise sisteman

Argitalpen data: 2020/08/26

Garrantzia: Txikia

Kaltetutako baliabideak:

OpenEnterprise bertsio guztiak 3.3.5 bertsiora arte.

Azalpena:

Kaspersky erakundeko Roman Lozko ikertzaileak ahultasun bat atzeman du Emersonen OpenEnterprise sisteman erabilitako zifratzean. Horren bidez, erasotzaile batek OpenEnterprisek erabilitako kredentzialak lortu litzake, gailu eta kanpo sistemetara sartzeko.

Konponbidea:

OpenEnterprise 3.3 Service Pack 6 (3.3.6) instalatzea gomendatzen da. Eskuragarri dago Emersonen laguntza orrian.

Xehetasuna:

Atzemandako ahultasuna OpenEnterpriseko zifratze desegoki bati dagokio; horrek bere kredentzialak lortzeko aukera emango luke. Gainera, erasotzaile batek erraz lor litzake kredentzial horiek, ahultasun horren ondorioz. Ahultasun horretarako, CVE-2020-16235 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, SCADA, Ahultasuna.

Hainbat ahultasun Red Lion etxearen N-Tron 702-W

eta N-Tron 702M12-W sistemetan

Argitalpen data: 2020/08/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- N-Tron 702-W, bertsio guztiak;
- N-Tron 702M12-W, bertsio guztiak.

Azalpena:

Thomas Weber, SEC Consult Vulnerability Lab erakundeko ikertzaileak, 5 ahultasun atzeman ditu; 3 larritasun kritikokoak eta 2 larritasun handikoak. Motak: XSS, CSRF, dokumentatu gabeko funtzionalitatea (backdoor) eta hirugarrenen osagaiak mantenimendurik gabe erabiltzea

Konponbidea:

Red Lion 702-W serieko produktu guztiak jarraitutasunik gabeko produktu izatera pasa ziren 2018an, eta ezin dira eguneratu. Fabrikatzaileak gomendatzen du produktu horiek sare seguru baten modu lokalean erabiltzea.

Xehetasuna:

- Kaltetutako produktua gailuan dagoen interfaze ez dokumentatu baten mende dago. Horrela izanik, erasotzaile batek *root* pribilegioekin exekutatu litzake komandoak gailuan. Ahultasun horretarako, CVE-2020-16204 identifikatzailea erreserbatu da.
- Kaltetutako produktua islatutako XSS (*Cross-Site Scripting*) baten mende dago. Horren ondorioz, erasotzaile batek kode arbitrarioa exekutatu lezake urrunetik, eta erasotutako erabiltzailearen testuinguruan ekintzak burutu. Ahultasun horretarako, CVE-2020-16210 identifikatzailea erreserbatu da.
- Kaltetutako produktua biltegiratutako XSS (*Cross-Site Scripting*) baten mende dago. Horren ondorioz, erasotzaile batek kode arbitrarioa exekutatu lezake urrunetik, datu konfidentzialetarako sarbidea lortzeko. Ahultasun horretarako, CVE-2020-16206 identifikatzailea erreserbatu da.
- Kaltetutako produktua CSRF (*Cross-Site Request Forgery*) baten mende dago; horren ondorioz, erasotzaile batek gailu baten hainbat konfigurazio alda litzake, baimendutako erabiltzaile bat engainatuz, bereziki diseinatutako lotura batera sartzeko. Ahultasun horretarako, CVE-2020-16208 identifikatzailea erreserbatu da.
- Kaltetutako produktua ahula da software zaharkitua duten hirugarrenen osagaiak erabiltzeagatik. Horren ondorioz, erasotzaile batek informazio konfidentziala lortu lezake, eta gailuaren kontrola bereganatu. Ahultasun horretarako, CVE-2017-16544 identifikatzailea erreserbatu da.

Etiketak: Komunikazioa, Azpiegitura kritikoak, Ahultasuna