2019ko Abenduaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Hainbat ahultasun Moxa-ren AWK-3121-en

Argitalpen data: 2019/12/02

Garrantzia: Kritikoa

Kaltetutako baliabideak:

AWK-3121 Series, 1.14 bertsioa eta lehenagokoak.

Azalpena:

Samuel Huntley ikertzaileak Moxa-ren AWK-3121 serieari eragiten dioten hainbat ahultasun aurkitu ditu. Horiek baliatuz, urruneko erasotzaile batek kodea exekuta lezake, komandoak injektatu, Cross-Site Scripting egin, kredentzialak kudeatu, sarbidearen kontrol okerra eta Cross-Site Request Forgery (CSRF).

Konponbidea:

Fabrikatzailea konponbide bat prestatzen ari da. Informazio gehiago eskuratzeko jarri harremanetan zerbitzuarekin.

Xehetasuna:

- Elementu berezien neutralizazio desegokia baliatuz, erasotzaile batek komandoak injekta litzake shell metakaraktereen bidez hainbat parametrotan. Ahultasun horretarako CVE-2018-10697, CVE-2018-10699 eta CVE-2018-10702 identifikatzaileak erabili dira.
- Sarrera parametroen neutralizazio desegokia baliatuz, erasotzaile batek cookieak lapurtu litzake parametro zehatzean XSS erabiliz. Ahultasun horretarako CVE-2018-10692 eta CVE-2018-10700 identifikatzaileak erabili dira.
- Memoriaren bufferraren mugen barnean eragiketen murrizpen desegokia baliatuz, erasotzaile batek bufferraren gainezkatzea eragin lezake gailuaren hainbat parametrotan. Ahultasun horretarako CVE-2018-10693, CVE-2018-10695, CVE-2018-10701 eta CVE-2018-10703 identifikatzaileak erabili dira.
- Erasotzaile batek gailuaren kredentzialak eskura litzake hauetako ahultasunen bat baliatuz:
  - gailuak HTTP trafikoa modu lehenetsian onartzen du, horrela komunikazio bide ez-seguru bat eskainiz erabiltzailea web zerbitzarira konektatzeko. Ahultasun horretarako CVE-2018-10690 identifikatzailea erabili da.
  - irekita dagoen eta modu lehenetsian inolako zifratze neurririk ez duen Wi-Fi konexio bat eskaintzen du gailuak. Ahultasun horretarako CVE-2018-10694 identifikatzailea erabili da.
  - gailuak zifratu gabeko TELNET zerbitzu bat eskaintzen du modu lehenetsian. Ahultasun horretarako CVE-2018-10698 identifikatzailea erabili da.
- Erasotzaile batek sarbidea eskura lezake baimenik gabe systemlog.log deskargatuz. Ahultasun horretarako CVE-2018-10691 identifikatzailea erabili da.
- Web interfazea ez dago babestuta CSRF erasoen aurrean, eta hori baliatuz erasotzaile batek faltsututako eskaerak egin litzake. Ahultasun horretarako CVE-2018-10696 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Komatxo artean jarri gabeko elementua edo bilaketa bidea Reliable Controls-en LicenseManager-en

Argitalpen data: 2019/12/04

Garrantzia: Altua

Kaltetutako baliabideak:

RC-LicenseManager, 3.4 eta lehenagoko bertsioak.

Azalpena:

Applied Risk-eko Gjoko Krstic-ek komatxo artean jarri gabeko elementu edo bilaketa bide erako ahultasun baten berri eman zuen, Reliable Controls-en LicenseManager produktuari eragiten diona.

Konponbidea:

Fabrikatzaileak RC-LicenseManager-en 3.5 bertsioa argitaratu du, RC-Studio-ren azken softwarearen barnean doana. Reliable Controls-ek erabiltzaileei gomendatzen die RC Studio 3.6.3 bertsiora eguneratzea.

Xehetasuna:

Autentifikatutako erabiltzaile batek asmo gaiztoko kodea txerta lezake sistemaren erroaren bidean, eta hori baliatuz kodea exekuta lezake aplikazioaren pribilegio altuekin. Ahultasun hori arrakastaz baliatuz gero, erasotzaile batek sistema blokea lezake, datu konfidentzialak ikusi, edo komando arbitrarioak exekutatu. Ahultasun horretarako CVE-2019-18245 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Loturaren ebazpen desegokia Thales DISen SafeNet Sentinel LDK License Manager Runtime-n

Argitalpen data: 2019/12/10

Garrantzia: Altua

Kaltetutako baliabideak:

SafeNet Sentinel LDK License Manager, 7.101 baino lehenagoko bertsio guztiak (soilik Microsoft Windows duten bertsioak).

Azalpena:

Blizzard Entertainment Red Team-eko Ryan Wincey ikertzaileak kritikotasun altuko ahultasun baten berri eman du. Hori baliatuz erasotzaile lokal batek pribilegioen eskalatzea egin lezake.

Konponbidea:

Thales-ek 7.101 bertsiora edo berriago batera eguneratzea gomendatzen du.

Xehetasuna:

Kaltetutako produktua ahula da zerbitzu modura konfiguratzen denean. Ahultasun hori baliatuz, sarbide lokala lukeen erasotzaile batek sistemaren direktorioko fitxategiak idatzi eta ezaba litzake lotura sinbolikoak erabiliz, eta horren ondorioz pribilegioen eskalatzea egin liteke. Ahultasun hori asmo gaiztoko DLLak exekutatzeko ere balia liteke, eta horrek negatiboki eragin lezake sistemaren integritatean eta eskuragarritasunean. Ahultasun horretarako CVE-2019-18232 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Pribilegioen eskalatzea General Electric-en HMI/SCADA iFIX-en

Argitalpen data: 2019/12/10

Garrantzia: Altua

Kaltetutako baliabideak:

GE Digital HMI/SCADA iFIX, 6.1 eta lehenagoko bertsioak.

Azalpena:

Applied Risk-eko ikertzaileek hainbat ahultasun aurkitu dituzte GE Digital-en HMI/SCADA iFIX produktuan.

Konponbidea:

GE Digital-ek produktu honen hedapen seguru bat egiteko argibideak eskaintzen ditu bere bezeroaren arreta zentroan.

Xehetasuna:

Pribilegioen eskalatze erako bi ahultasun aurkitu dira GE Digital-en HMI/SCADA iFIX produktuan. Horiek baliatuz erasotzaile batek sistema alda lezake eta kodearen exekuzio arbitrarioa eragin. Ahultasun horiek soilik balia daitezke erasotzailea autentifikatuta badago.

Etiketak: SCADA, Ahultasuna

Hainbat ahultasun Weidmueller-en produktuetan

Argitalpen data: 2019/12/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Ondoko produktuen 3.6.6 16102415 eta lehenagoko bertsioak:
  - IE-SW-VL05M-5TX,
  - IE-SW-VL05MT-5TX,
  - IE-SW-VL05M-3TX-2SC,
  - IE-SW-VL05MT-3TX-2SC,
  - IE-SW-VL05M-3TX-2ST,
  - IE-SW-VL05MT-3TX-2ST.
- Ondoko produktuen 3.5.2 16102415 eta lehenagoko bertsioak:
  - IE-SW-VL08MT-8TX,
  - IE-SW-VL08MT-5TX-3SC,
  - IE-SW-VL08MT-5TX-1SC-2SCS,
  - IE-SW-VL08MT-6TX-2ST,
  - IE-SW-VL08MT-6TX-2SC,
  - IE-SW-VL08MT-6TX-2SCS.
  - Ondoko productuen3.3.8 16102416 eta lehenagoko bertsioak
  - IE-SW-PL08M-8TX,
  - IE-SW-PL08MT-8TX,
  - IE-SW-PL08M-6TX-2SC,
  - IE-SW-PL08MT-6TX-2SC,
  - IE-SW-PL08M-6TX-2ST,
  - IE-SW-PL08MT-6TX-2ST,
  - IE-SW-PL08M-6TX-2SCS,
  - IE-SW-PL08MT-6TX-2SCS.
- Ondoko produktuen 3.3.16 16102416 eta lehenagoko bertsioak:
  - IE-SW-PL10M-3GT-7TX,
  - IE-SW-PL10MT-3GT-7TX,
  - IE-SW-PL10M-1GT-2GS-7TX,
  - IE-SW-PL10MT-1GT-2GS-7TX.
- Ondoko produktuen 3.4.2 16102416 eta lehenagoko bertsioak:
  - IE-SW-PL16M-16TX,
  - IE-SW-PL16MT-16TX,
  - IE-SW-PL16M-14TX-2SC,
  - IE-SW-PL16MT-14TX-2SC,
  - IE-SW-PL16M-14TX-2ST,
  - IE-SW-PL16MT-14TX-2ST.
- Ondoko produktuen 3.4.4 16102416 eta lehenagoko bertsioak:
  - IE-SW-PL18M-2GC-16TX,
  - IE-SW-PL18MT-2GC-16TX,
  - IE-SW-PL18M-2GC14TX2SC,
  - IE-SW-PL18MT-2GC14TX2SC,
  - IE-SW-PL18M-2GC14TX2ST,
  - IE-SW-PL18MT-2GC14TX2ST,
  - IE-SW-PL18M-2GC14TX2SCS,
  - IE-SW-PL18MT-2GC14TX2SCS.
- Ondoko produktuen 3.3.4 16102416 eta lehenagoko bertsioak:
  - IE-SW-PL09M-5GC-4GT,
  - IE-SW-PL09MT-5GC-4GT.

Azalpena:

 hainbat ahultasun aurkitu ditu Weidmueller-en switch industrialetan. Horiek baliatuz urruneko erasotzaile batek gailura baimenik gabeko sarbidea lor lezake, bere konfidentzialtasun, integritate eta eskuragarritasunari eraginez.

Konponbidea:

 eta Weidmueller-ek ondoko arintze neurriak proposatzen dituzte:

- CVE-2019-16672 ahultasunerako konponbideak:
  - IE-SW-VL05M, IE-SW-VL08MT Series;
    - Firmwarearen eguneraketa instalatzea.
  - IE-SW-PL08M, IE-SW-PL10M, IE-SW-PL16M, IE-SW-PL18M, IE-SW-PL09M Series:
    - Ez da beharrezkoa firmwarea eguneratzea, posible baita zifratua konfiguratzea 'https only' aukera hautatuz.
- CVE-2019-16670, CVE-2019-16671, CVE-2019-16673 eta CVE-2019-16674 ahultasunetarako konponbideak:
  - IE-SW-VL05M, IE-SW-VL08MT, IE-SW-PL08M, IE-SW-PL10M, IE-SW-PL16M, IE-SW-PL18M, IE-SW-PL09M serieak;
    - Firmwarearen eguneraketa instalatzea.

Xehetasuna:

- Gailua ez dago konfiguratuta indar hutseko erasoei aurre egiteko. Hori baliatuz erasotzaile batek gailura sartzeko kredentzialak eskura litzake. Ahultasun horretarako CVE-2019-16670 identifikatzailea erabili da.
- Urrunetik autentifikatzen diren erabiltzaileek gailuak funtzionatzeari uztea eragin dezakete, bereziki diseinatutako pakete bat bidaliz gero. Ahultasun horretarako CVE-2019-16671 identifikatzailea erabili da.
- Kredentzialen moduko datu sentikorrak testu lauan transmititzen dira, eta horregatik erasotzaile batek errazki eskura litzake. Ahultasun horretarako CVE-2019-16672 identifikatzailea erabili da.
- Pasahitzak testu lauan gordetzen dira, eta gailura sarbidea lukeen erasotzaile batek irakur litzake. Ahultasun horretarako CVE-2019-16673 identifikatzailea erabili da.
- Cookie batean erabiltzen den autentifikazioari buruzko informazioa erraz asma daiteke eta pasahitzak arriskuan jar litezke sarean atzemanez gero. Ahultasun horretarako CVE-2019-16674 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Siemens produktuetan

Argitalpen data: 2019/12/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SPPA-T3000 Application Server, bertsio guztiak,
- SPPA-T3000 MS3000 Migration Server, bertsio guztiak,

- EN 100 Ethernet modulua,
  - IEC 61850 aldaera, V4.37 baino lehenagoko bertsio guztiak,
  - PROFINET IO aldaera, bertsio guztiak,
  - Modbus TCP aldaera, bertsio guztiak,
  - DNP3 aldaera, bertsio guztiak,
  - IEC 104 aldaera, bertsio guztiak.
- XHQ, V6.0.0.2 bertsioaren aurreko guztiak,
- SCALANCE W1700, V1.1 bertsioa baino lehenagoko guztiak,
- SCALANCE W700, V6.4 bertsioa baino lehenagoko guztiak,
- SiNVR 3 Central Control Server (CCS), bertsio guztiak,
- SiNVR 3 Video Server, bertsio guztiak,
- RUGGEDCOM ROS:
-
  - RMC8388, bertsio guztiak,
  - RSG2488, bertsio guztiak,
  - RSG920P, bertsio guztiak,
  - RSG9xx R/C, bertsio guztiak,
  - RSL910, bertsio guztiak,
  - RST2228, bertsio guztiak.

Azalpena:

Siemensek hainbat ahultasun aurkitu ditu bere gailu batzuetan. Urruneko erasotzaile batek informazioa eman lezake ezagutzera, pribilegioen eskalatzea egin, bideak saihestu, kode arbitrarioa exekutatu, zerbitzuaren ukapen egoera eragin edo datuak injektatu.

Konponbidea:

Siemensek hainbat eguneraketa argitaratu ditu, kaltetutako gailuaren arabera:

- SPPA-T3000 Application Server, Service Pack R8.2 SP1 partxea aplikatzea.
- Módulo EN 100 Ethernet, IEC 61850 aldaera, V4.37 bertsiora eguneratzea.
- XHQ, V6.0.0.2 bertsiora eguneratzea.
- SCALANCE W1700, V1.1 bertsiora eguneratzea.
- SCALANCE W700, V6.4 bertsiora eguneratzea.

Kaltetutako gainerako produktuen kasuan, Siemens-en ohartarazpen ofizialetako *Workarounds and Mitigations* ataleko gomendioak kontsultatzea.

Xehetasuna:

Ondoren zehazten dira ahultasun kritikoak:

- Autentifikazio desegokia. Ahultasun horietarako CVE-2019-18337, CVE-2019-18284, CVE-2019-18314, CVE-2019-18315, CVE-2019-18321 eta CVE-2019-18322 identifikatzaileak esleitu dira.
- Autentifikazio falta funtzio kritikoan. Ahultasun horretarako CVE-2019-18339 identifikatzailea erabili da.
- Funtzioaren edo metodo arriskutsuaren agerpena. Ahultasun horretarako CVE-2019-18342 identifikatzailea erabili da.
- Fidagarriak ez diren datuen deserializazioa. Ahultasun horietarako CVE-2019-18283 eta CVE-2019-18316 identifikatzaileak erabili dira.
- Egiaztapen falta fitxategiak igotzean. Ahultasun horretarako CVE-2019-18313 identifikatzailea erabili da.
- Memoria dinamikoan (Heap) oinarritutako bufferraren gainezkatzea. Ahultasun horietarako CVE-2019-18323, CVE-2019-18324, CVE-2019-18325, CVE-2019-18326, CVE-2019-18327, CVE-2019-18328, CVE-2019-18329, CVE-2019-18330, CVE-2019-18289 eta CVE-2019-18293 identifikatzaileak erabili dira.

Gainerako ahultasunetarako identifikatzaile hauek esleitu dira: CVE-2019-13942, CVE-2019-13943, CVE-2019-13944, CVE-2018-14526, CVE-2019-13947, CVE-2019-18338, CVE-2019-18340, CVE-2019-18341, CVE-2018-18440, CVE-2019-13103, CVE-2019-13930, CVE-2019-13931, CVE-2019-13932, CVE-2018-4832, CVE-2019-18285, CVE-2019-18286, CVE-2019-18287, CVE-2019-18288, CVE-2019-18290, CVE-2019-18291, CVE-2019-18292, CVE-2019-18294, CVE-2019-18295, CVE-2019-18296, CVE-2019-18297, CVE-2019-18298, CVE-2019-18299, CVE-2019-18300, CVE-2019-18301, CVE-2019-18302, CVE-2019-18303, CVE-2019-18304, CVE-2019-18305, CVE-2019-18306, CVE-2019-18307, CVE-2019-18308, CVE-2019-18309, CVE-2019-18311, CVE-2019-18312, CVE-2019-18317, CVE-2019-18318, CVE-2019-18319, CVE-2019-18320, CVE-2019-18331, CVE-2019-18332, CVE-2019-18333, CVE-2019-18334 eta CVE-2019-18335.

Etiketak: Eguneraketa, Siemens, Ahultasuna

Hainbat ahultasun Schneider Electric-en produktuetan

Argitalpen data: 2019/12/11

Garrantzia: Altua

Kaltetutako baliabideak:

- Modicon:
  - M580, V2.80 bertsioaren aurreko guztiak,
  - M340, V3.01 bertsioaren aurreko guztiak,
  - Premium, V3.20 baino lehenagoko bertsio guztiak,
  - Quantum, V3.60 baino lehenagoko bertsio guztiak.
- EcoStruxure™ Control Expert V14.0 eta Unity Pro-ren bertsio guztiak (lehenago EcoStruxure™ Control Expert deitua).
- Saitel DP (866e), 11.06.08 baino lehenagoko bertsio guztiak.
- Saitel DR (HUe), 11.06.08 baino lehenagoko bertsio guztiak.
- Power SCADA, eta horri lotutako eguneraketa pilatzaileak barne:
-
  - Operation 9.0,
  - Expert 8.2,
  - Expert 8.1,
  - Expert 8.0,
  - Expert 7.4,
  - Expert 7.3.
- ClearSCADA 2017, 2017 R3 eta 2017 R2.

Azalpena:

Schneider-ek bost ahultasun aurkitu ditu, hiru kritikotasun altukoak, bat ertainekoa eta beste bat baxukoa, Schneider Electric-en hainbat gailuri eragiten dietenak.Urruneko erasotzaile batek zerbitzuaren ukapen egoera eragin lezake, autentifikazioa saihestu, kode arbitrarioa exekutatu edo sistemaren fitxategietan aldaketak egin.

Konponbidea:

Kaltetutako produktuetarako hainbat eguneratze eta arintze argitaratu ditu Scheneider-ek. Informazio gehiago eskuratzeko erreferentzien atala irakurri.

Xehetasuna:

- Kontrolatzailean baldintza bereziak edo ezohikoak daudenean egiten den egiaztatze baten ondorioz, ModbusTCP erabiliz, memoriaren bloke zehatzak edo baliogabeko indizeak dituzten datuak irakurtzean, erasotzaile lokal batek zerbitzuaren ukapen egoera eragin lezake kontrolatzailean. Ahultasun horretarako CVE-2019-6857, CVE-2019-6856 eta CVE-2018-7794 identifikatzaileak erreserbatu dira.
- Ahultasun hau baliatuz EcoStruxure Control Expert eta kontrolatzailearen arteko autentifikazio prozesua saihets liteke. Ahultasun horretarako CVE-2019-6855 identifikatzailea erreserbatu da.
- Bufferra kopiatzean sarreraren tamaina egiaztatzen ez denez, haren gainezkatzea eragin liteke. Erasotzaile lokal batek gehiegizko errekurtsibitatea duen asmo gaiztoko sarrera bat erabil lezake. Ahultasun horretarako CVE-2019-6858 identifikatzailea erreserbatu da.
- ClearSCADAren barneko karpeta batean baimenen, pribilegioen eta sarbide kontrolen egiaztapenean dauden akatsen ondorioz, pribilegio baxuak lituzkeen erabiltzaile batek datu baseak, ezarpenak eta ziurtagiriak ezabatu edo alda litzake. Ahultasuna baliatu ahal izateko, erabiltzaile horiek sarbidea izan behar dute sistema eragile horren fitxategien sistemara. Ahultasun horretarako CVE-2019-6854 identifikatzailea erabili da.

Etiketak: Eguneraketa, Schneider Electric, Ahultasuna

Pilan oinarritutako bufferraren gainezkatzea Advantech-en WebAcces/SCADAn

Argitalpen data: 2019/12/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Advantech WebAccess/SCADA, 8.4.2 bertsioa

Azalpena:

Tenablek pilan oinarritutako bufferraren gainezkatze erako (stack) ahultasun bat aurkitu du. Autentifikatu gabeko urruneko erasotzaile batek datu kopuru handi bat bidal lezake pilaren (stack) bufferrak gainezka egiteko.

Konponbidea:

8.4.3 bertsiora eguneratzea.

Xehetasuna:

CVE-2019-3975 kodearekin identifikatutako ahultasuna antzemateko Nessus-en *plugin* bat garatzen ari zela, Tenable-k autentikatu gabeko urruneko pilaren gainezkatze erako beste ahultasun bat aurkitu zuen Advantech WebAccess/SCADA produktuaren 8.4.2 bertsioan. *BwPAlarm.dll*-en *LogInfoFormat* funtzioak akats bat dauka, eta horren arrazoia da erabiltzaileak emandako datuen baliozkotze okerra, datuak tamaina finkoko pilaren buffer batera kopiatu aurretik, IOCTL 70533 RPC mezu bat prozesatzen denean. Ahultasun horretarako CVE-2019-3951 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, SCADA, Ahultasuna

Hainbat ahultasun Omron produktuetan

Argitalpen data: 2019/12/13

Garrantzia: Altua

Kaltetutako baliabideak:

- Omron PLC CJ series, bertsio guztiak.
- Omron PLC CS series, bertsio guztiak.
- Omron PLC NJ series, bertsio guztiak.

Azalpena:

Wang Zhibei eta n0b0dy ikertzaileek Omron gailuei eragiten dieten hainbat ahultasunen berri eman dute. Ahultasun horiek arrakastaz baliatuz gero, urruneko erasotzaile batek indar hutseko erasoak egin litzake sarbide kredentzialen aurka, baimendutako erabiltzaile bat balitz bezala sartu PLCaren egoerari buruzko informazioa eskuratzeko, edo baimenik gabeko sarbidea lortu FTP interfazera.

Konponbidea:

Omron-ek gomendatzen du ondoko neurriak hartzea ahultasunak arintzeko:

- FINS protokoloa iragaztea: PLCrako sarbidea suebaki baten bidez babestea, FINS protokolorako urruneko sarbidea blokeatuz, modu lehenetsian 9600 ataka duena.
- IP helbideak iragaztea: PLCrako sarbidea suebaki baten bidez babestea, konektatutako gailuak IP helbidearen bidez iragaziz.
- FTP protokoloa iragaztea: PLCrako sarbidea suebaki baten bidez babestea, FTP protokoloaren kontrako baimenik gabeko urruneko konexioak blokeatuz, modu lehenetsian 21 ataka duena.

Xehetasuna:

- Ahultasunak baliatuz urruneko erasotzaile batek honakoa egin lezake:
- mezuak faltsutzea (spoofing) edo komando arbitrarioak exekutatzea. Ahultasun horretarako CVE-2019-18259 identifikatzailea erreserbatu da.
- PLC eta kontrolatzailearen arteko trafikoa monitorizatzea eta ondoren balbula industrialak irekitzea edo ixtea eragin lezaketen mezuak errepikatzea. Ahultasun horretarako CVE-2019-13533 identifikatzailea erreserbatu da.
- kanpoko murrizpenik gabe blokeatzea. Softwareak ondo egiaztatzen du blokeo bat dagoen, baina hori kontrolpeko areatik kanpo dagoen erasotzaile batek kanpotik kontrola dezake. Ahultasun horretarako CVE-2019-18269 identifikatzailea erreserbatu da.
- indar hutseko erasoa. Autentifikazio saio akastunak saihesteko ez da ezartzen segurtasun neurri nahikorik. Ahultasun horretarako CVE-2019-18261 identifikatzailea erreserbatu da.

Etiketak: Komunikazioak, Ahultasuna

Hainbat ahultasun Advantech-en produktuetan

Argitalpen data: 2019/12/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- DiagAnywhere Server, 3.07.11 eta lehenagoko bertsioak;
- WebAccess, bertsio guztiak.

Azalpena:

Pilan oinarritutako bufferraren gainezkatze erako hainbat ahultasunen berri eman da. Horiek baliatuz erasotzaile batek urrunetik kodea exekuta lezake.

Konponbidea:

- DiagAnywhere Server: 3.07.14. bertsiora eguneratzea.
- WebAccess: oraingoz ez da eguneraketarik argitaratu.

Xehetasuna:

- TCP ataka entzunez fitxategien transferentzia zerbitzuan dauden pilan oinarritutako bufferraren gainezkatze erako hainbat ahultasun baliatuz, autentifikatu gabeko urruneko erasotzaile batek kode arbitrarioa exekuta lezake biktimaren pribilegio berdinekin. Ahultasun horretarako CVE-2019-18257 identifikatzailea erabili da.
- WebAccess-en BwOpcBs.exe exekutagarriak, webvrpcs zerbitzuan 0x2711 IOCTL-ren bidez sartzean, erabiltzailearen sarreraren luzeraren baliozkotze falta dauka, tamaina finkoko buffer batera kopiatua izan aurretik. Hori baliatuz erasotzaile batek kodea exekuta lezake administratzaile baimenekin.

Etiketak: 0day, Eguneraketa, Ahultasuna

Hainbat ahultasun WAGOren produktuetan

Argitalpen data: 2019/12/17

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Series PFC100 (750-81xx/xxx-xxx).
- Series PFC200 (750-82xx/xxx-xxx).
- 750-852, 750-831/xxx-xxx, 750-881, 750-880/xxx-xxx, 750-889.
- 750-823, 750-832/xxx-xxx, 750-862, 750-890/xxx-xxx, 750-891

Azalpena:

Cisco Talos-eko Kelly Leuschner-ek WAGOren gailuei eragiten dieten 9 ahultasunen berri eman du, 8 larritasun kritikokoak eta bat kritikotasun ertainekoa. Ahultasun horiek arrakastaz baliatuz gero urruneko erasotzaile batek gailuaren konfigurazioa manipulatu lezake edo bere oinarrizko funtzioak aldatu, aldatutako IP paketeen bidez. Horrela gailuaren kontrola har liteke.

Konponbidea:

- WAGOk ondoko ekintzak egitea gomendatzen du:
  - Gailuen firmwarea 15. bertsiora edo berriago batera eguneratzea.
  - 6626 ataka desgaitzea gailuaren hasierako instalazioaren eta konfigurazioaren ondoren, prozesu horietan soilik erabiltzen baita.

Xehetasuna:

Ondoren zehazten da zein diren ahultasun kritikoak. Horiek baliatuz urruneko erasotzaile batek ondoko ekintzak egin litzake:

- Bufferraren gainezkatzea. Ahultasun horietarako CVE-2019-5079, CVE-2019-5081 eta CVE-2019-5082 identifikatzaileak erreserbatu dira.
- Funtzio kritikoetarako ez autentifikatzea. Ahultasun horietarako CVE-2019-5077, CVE-2019-5078 eta CVE-2019-5080 identifikatzaileak erreserbatu dira.
- Bufferrera sarbidea tamainaren balio okerrarekin. Ahultasun horietarako CVE-2019-5074 eta CVE-2019-5075 identifikatzaileak erreserbatu dira.

Kritikotasun ertaineko ahultasuna baliatuz urruneko erasotzaile batek informazioa ezagutzera eman lezake datuak bidaliz. Ahultasun horretarako CVE-2019-5073 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun ABBren PB610 Panel Builder 600-en

Argitalpen data: 2019/12/17

Garrantzia: Altua

Kaltetutako baliabideak:

- PB610 Panel Builder 600, 2.8.0.424 eta lehenagoko bertsioak.

Azalpena:

NSFOCUSeko ikertzaileek hainbat ahultasunen berri eman dute. Horiek baliatuz urruneko erasotzaile batek gailua geldiarazi lezake edo eskuraezin utzi, sistemaren nodoaren kontrola hartu edo kode arbitrarioa injektatu.

Konponbidea:

- 2.8.0.460 bertsiora eguneratzea;
- Aplikazioaren PB610 direktorioan dauden DLL fitxategiak ezabatzea.

Xehetasuna:

- Fitxategiaren luzera egiaztatzen ez denez, HMIStudio osagaia blokeatu egiten da aplikazioaren *.JPR fitxategi huts bat kargatzen saiatzean. Hori baliatuz erasotzaile batek gailuan zerbitzuaren ukapen egoera eragin lezake. Ahultasun horretarako CVE-2019-18994 identifikatzailea erabili da.
- HMISimulator panelak huts egiten du HTTP eskarien luzera baliozkotzean. Hori baliatuz erasotzaile batek zerbitzuaren ukapen egoera eragin lezake bereziki manipulatutako HTTP paketeak bidaliz. Ahultasun horretarako CVE-2019-18995 identifikatzailea erabili da.
- HMIStudio-k programaren direktoriotik kanpo dauden DLL fitxategiak onartzen ditu. Hori baliatuz, sarbide lokala lukeen erasotzaile batek kodea exekuta lezake asmo gaiztoko DLL fitxategien bidez. Ahultasun horretarako CVE-2019-18996 identifikatzailea erabili da.
- HMISimulator osagaiak irakurketa/idazketa interfazea erabiltzen du fitxategiak manipulatzeko. Hori baliatuz erasotzaile batek laneko direktoriotik kanpoko fitxategietara sarbidea lor lezake baimenik gabe. Ahultasun horretarako CVE-2019-18997 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Cross-site Scripting GEren Fast Switch 61850-en

Argitalpen data: 2019/12/18

Garrantzia: Ertaina

Kaltetutako baliabideak:

GE S2020/S2020G Fast Switch 61850, 07A03 eta lehenagoko bertsioak.

Azalpena:

Biznet Bilisim A.S.-ko Murat Aydemir-ek GEren gailuei eragiten dien ahultasun baten berri eman du. Urruneko erasotzaile batek kode arbitrarioa injekta lezake edo datu konfidentzialak hedatzea ahalbidetu.

Konponbidea:

GEk gomendatzen du gailuak 07A04 bertsiora edo berriago batera eguneratzea.

Xehetasuna:

Urruneko erasotzaile batek Javascript kode arbitrarioa injekta lezake bereziki diseinatutako HTTP pakete batean, eta hori islatu egingo litzateke HTTPren erantzunean. Gailua ahula da, era berean, biltegiratutako Cross-Site Scripting (XSS) erasoen aurrean. Hori baliatuz, urruneko erasotzaile batek saioa bahitu lezake, datu sentikorrak agerian utzi, Cross-Site Request Forgery (CSRF) eragin edo kodea urrunetik exekutatu. Ahultasun horretarako CVE-2019-18267 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Kontrolatu gabeko bilaketa bidea Sprecher Automation-en SPRECON-V460-en

Argitalpen data: 2019/12/18

Garrantzia: Altua

Kaltetutako baliabideak:

SPRECON-V460.

Azalpena:

Sprecher Automation-en SPRECON-V460 gailuari eragiten dion ahultasun baten berri eman da. Ahultasun hori arrakastaz baliatuz gero,

erasotzaile batek asmo gaiztoko DLLak karga litzake eta kodea exekutatu.

Konponbidea:

Sprecher Automation-ek gailuak eguneratzea gomendatzen du 7.50 bertsiotik aurrera, eta SPRECON-V460-en editoretik lehenetsitako .wp6 fitxategiak ez exekutatzea gomendatzen du.

Xehetasuna:

Erasotzaile batek lor lezake gailuak asmo gaizto DLL fitxategiak kargatzea, fitxategiak aldatzeko eta kodea exekutatzeko administratzaile pribilegioak behar ez diren direktorio batetik. Ahultasuna gertatzen da SPRECON-V460-ek bide horretatik .wsp6 fitxategia irekitzen duenean. Ahultasun horretarako CVE-2019-15638 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun CODESYSen produktuetan

Argitalpen data: 2019/12/19

Garrantzia: Ertaina

Kaltetutako baliabideak:

- CODESYS SP Realtime NT, v2.3.7.28 baino lehenagoko bertsioak;
- CODESYS Runtime Toolkit 32 bit full, v2.4.7.54 baino lehenagoko bertsioak;
- CODESYS PLCWinNT, v2.4.7.54 baino lehenagoko bertsioak.

Azalpena:

NSFOCUSeko Chen Jie-k CODESYSen gailuei eragiten dien kritikotasun ertaineko ahultasun baten berri eman du. Urruneko erasotzaile batek zerbitzuaren ukapen egoera eragin lezake.

Konponbidea:

3S-Smart Software Solutions GmbH-k ahultasun horiek konpontzen dituzten ondoko bertsioak argitaratu ditu. Eguneraketak eskuratzeko CODESYSen webguneko eguneraketen atala bisitatu beharra dago:

- CODESYS SP Realtime NT, v2.3.7.28 bertsiora eguneratzea.
- CODESYS Runtime Toolkit 32 bit full, v2.4.7.54 bertsiora eguneratzea.
- CODESYS PLCWinNT, v2.4.7.54 bertsiora eguneratzea.

Xehetasuna:

Bereziki sortutako eskaera batek, zerbitzarira bidalita, NULL erakuslearen deserreferentzia eragin lezake. Urruneko erasotzaile batek zerbitzuaren ukapen egoera eragin lezake. Eskaera hori soilik prozesatzen da kontrolatzailean inolako pasahitzik ez bada konfiguratu, edo aldez aurretik erasotzaileak autentifikatzea lortu badu. Ahultasun horretarako CVE-2019-19789 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Zifratze desegokia Philips-en Dual WAN router osasun gailuetan

Argitalpen data: 2019/12/20

Garrantzia: Ertaina

Kaltetutako baliabideak:

Dual Wan routerra duten osasun gailuak:

- Veradius Unity (718132), 2016 eta 2018ko abuztu bitartean saldutakoak, haririk gabeko edo ViewForum aukera dutenak;
- Pulsera (718095) eta Endura (718075), 2017ko ekainaren 26tik 2018ko abuztuaren 7ra bitartean saldutakoak, haririk gabeko edo ViewForum aukera dutenak.

Azalpena:

New York-eko Ospitale Presbiterianoko Daniel Yagudayev-ek Philips-en osasun gailuei eragiten dien kritikotasun ertaineko ahultasun baten berri eman du. Alboko erasotzaile batek haririk gabeko datuen transferentzia arriskuan jar lezake.

Konponbidea:

Philipsek konponbide bat dauka bere produktuetan haririk gabeko edo ViewForum aukerak dituzten erabiltzaileentzat, Dual WAN routerraren konfigurazioa eguneratzeko. Hori eskuratzeko Philips-en bezezoaren arreta zerbitzuarekin harremanetan jarri beharra dago.

Xehetasuna:

Dual WAN routerraren softwareak beharrezkoa duen babes mailarako zifratze ahuleko eskema bat erabiltzen du. Alboko erasotzaile batek haririk gabeko datuen transferentzia arriskuan jar lezake. Ahultasun horretarako CVE-2019-18263 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Osasuna, Ahultasuna

Zerbitzuaren ukapen erako ahultasuna Moxaren

produktuetan

Argitalpen data: 2019/12/20

Garrantzia: Altua

Kaltetutako baliabideak:

- EDS-G508E Series, 6.0 bertsioa eta lehenagokoak.
- EDS-G512E Series, 6.0 bertsioa eta lehenagokoak.
- EDS-G516E Series, 6.0 bertsioa eta lehenagokoak.

Azalpena:

Yuval Ardon eta Matan Dobrushin-ek ahultasun baten berri eman dute. Hori baliatuz erasotzaile batek kaltetutako produktuen zerbitzuaren ukapen egoera eragin lezake.

Ebazpena:

Moxaren zerbitzu teknikoaren zentroan eskuragarri dagoen eguneraketa ezartzea.

Xehetasuna:

PROFINET DCE-RPCren diagnostiko paketeek zerbitzuaren ukapen egoera eragin lezakete kaltetutako produktuetan. Ahultasun horretarako CVE-2019-19707 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Pilan oinarritutako bufferraren gainezkatzea WECONen PLC Editor-en

Argitalpen data: 2019/12/20

Garrantzia: Altua

Kaltetutako baliabideak:

PLC Editor, 1.3.5_20190129 bertsioa.

Azalpena:

Trend Micro's Zero Day Initiative-ko Francis Provencher (PRL) eta Natnael Samson-ek (Natti) pilan oinarritutako bufferraren gainezkatze erako (stack) ahultasunaren berri eman dute.

Konponbidea:

WECON konponbide bat garatzen ari da. Informazio gehiago eskuratzeko WECONen zerbitzu webgunearekin harremanetan jarri.

Xehetasuna:

Erasotzaile batek pilan oinarritutako bufferraren gainezkatze erako (stack) ahultasuna balia lezake, bereziki diseinatutako proiektu fitxategi bat erabiliz, aplikazioaren pribilegioekin kodea exekutatzeko. Ahultasun horretarako CVE-2019-18236 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna

Cross-Site Scripting erako ahultasuna Reliable Controls produktuetan

Argitalpen data: 2019/12/20

Garrantzia: Altua

Kaltetutako baliabideak:

- MACH-ProWebSys eta MACH-ProWebCom, 2.15 baino lehenagoko bertsio guztiak (firmwarearen 8.26.4 bertsioa baino lehenagokoak).

Azalpena:

Applied Risk-eko Gjoko Krstic-ek Reliable Controls-en gailuei eragiten dien ahultasun baten berri eman du. Hori baliatuz urruneko erasotzaile batek komandoak exekuta litzake kaltetutako erabiltzailearen izenean.

Ebazpena:

MACH-ProWebCom/Sys firmware revisión 8.26.4 bertsiora eguneratu.

Xehetasuna:

Autentifikatutako erabiltzaile batek asmo gaiztoko lotura batean klikatuko balu, erasotzaile batek hori balia lezake kaltetutako erabiltzailearen izenean komandoak exekutatzeko. Ahultasun horretarako CVE-2019-18249 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

CSRF erako ahultasuna eWON-en hainbat produktutan

Argitalpen data: 2019/12/26

Garrantzia: Altua

Kaltetutako baliabideak:

- Flexy, 14.0s0 baino lehenagoko bertsioak;
- Cosy, 14.0s0 baino lehenagoko bertsioak.

Azalpena:

Titanium Industrial Security-ko Ander Martinezek eWon gailuek duten ahultasun baten berri eman du. Hori baliatuz, urruneko erasotzaile batek CSRF eraso bat egin lezake, administratzailearen makina arriskuan jarriz.

Konponbidea:

14.0s0 bertsiora eguneratzea.

Xehetasuna:

- Erasotzaile batek CSRF eraso bat egin lezake gailuaren pasahitza aldatzeko edo administratzailearen makina arriskuan jartzeko, nabigatzailerako exploit-en bat erabiliz. Biktimak kredentzialak sartu behar ditu kodea exekutatu baino lehen.

Etiketak: Eguneraketa, Ahultasuna