2019ko Irailaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Saioaren finkapena BectonDickinson-en Pyxis ES-en

Argitalpen data: 2019/09/06

Garrantzia: Altua

Kaltetutako baliabideak:

- Pyxis Enterprise Server, 1.3.4tik 1.6.1era bitarteko bertsioak;
- Windows Server-dun Pyxis Enterprise Server, 4.4tik 4.12ra bitarteko bertsioak.

Azalpena:

BDk saioaren finkapen erako ahultasun baten berri eman du, Pyxis ES (Enterprise Server) ekipamenduari eragiten diona. Ahultasun hori arrakastaz baliatuz gero, erasotzaileak aldez aurretik autentifikatutako erabiltzaile baten saioa berrerabil lezake, eta horrela pribilegioen maila berdina lortuko luke, eta pazienteen osasun datuetara sartzeko aukera izan lezake.

Konponbidea:

Ahultasun hori konpontzeko BDk Pyxis Enterprise Server-en 1.6.1.1 bertsioa argitaratu du.

Xehetasuna:

Pyxis ES produktuak saioaren finkapen erako ahultasuna dauka, saioaren itxieraren kudeaketa oker baten ondorioz, domeinu kontrolatzaile baten bidez erabiltzaile bat autentifikatu denean. Ahultasun hori baliatuz, erasotzaile batek aldez aurretik sisteman erregistratutako erabiltzailearen saioa berrerabil lezake, eta horrela pribilegioak eskuratu eta gailura sartzea lortu. Ahultasun hori arrakastaz baliatuz gero, pazienteen datu konfidentzialetako informazio sentikorra eskura liteke. Ahultasun horretarako CVE-2019-13517 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Red Lion Controls-en Crimson-en

Argitalpen data: 2019/09/06

Garrantzia: Altua

Kaltetutako baliabideak:

- Crimson, 3.0 eta lehenagoko bertsioak;
- Crimson, 3.1 eta lehenagoko bertsioak, 3112.00 bertsiora arte.

Azalpena:

Red Lion Controls-en Crimson-en hainbat eratako ahultasunak aurkitu dira: memoriaren bufferraren murrizpen okerra, memoriako erakusleen kudeaketa okerra, aldez aurretik askatutako baliabideen berrerabilpena eta barneratutako gako kriptografikoen erabilpena. Horiek baliatuz urruneko erasotzaile batek kodea exekuta lezake, sistema blokeatu eta babestutako informaziora sarbidea lortu.

Konponbidea:

- Crimson 3.1 311200 bertsiora edo geroagoko batera eguneratzea.

Xehetasuna:

- Memoriako bufferreko eragiketen murrizpen oker bat baliatuz, urruneko erasotzaile batek kodea exekuta lezake. Ahultasun horretarako CVE-2019-10978 identifikatzailea erreserbatu da.
- Erakusleen kudeaketa oker bat baliatuz, erasotzaile batek bereziki diseinatutako fitxategi bat bidal lezake programak gaizki erabil ditzan erakusleak. Ahultasun horretarako CVE-2019-10984 identifikatzailea erreserbatu da.
- Produktuan barneratutako gako kriptografikoaren erabilpena baliatuz, erasotzaile batek konfigurazio fitxategietara sarbidea lor lezake. Ahultasun horretarako CVE-2019-10990 identifikatzailea erreserbatu da.
- Aldez aurretik askatutako baliabideen berrerabilpena baliatuz, erasotzaile batek, bereziki diseinatutako fitxategi baten bidez, aske eta aplikazioarentzat eskuraezin egon beharko lukeen memoriaren kokapen bati erreferentzia egin liezaioke, horrela kontrolatu gabeko memoriara sarbidea ahalbidetuz. Ahultasun horretarako CVE-2019-10994 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Osokoen gainezkatze erako ahultasuna OSIsoft-en PI SQL Client-en

Argitalpen data: 2019/09/11

Garrantzia: Altua

Kaltetutako baliabideak:

PI SQL Client 2018 (PI SQL Client OLEDB 2018).

Azalpena:

Osokoen gainezkatze erako ahultasun bat aurkitu da, OSIsoft-en PI SQL Client-en interfazearen osagaiari eragiten diona. Ahultasun hori arrakastaz baliatuz gero urruneko erasotzaile batek kodea exekuta lezake edo zerbitzuaren ukapen egoera sortu.

Konponbidea:

OSIsoft-ek gomendatzen du PI SQL Client 2018 R2 bertsiora edo geroagoko batera eguneratzea, OSIsoft-en bezeroaren atarian eskuragarri dagoena.

Xehetasuna:

Erasotzaile batek hirugarren batzuen osagaiaren ahultasun hori balia lezake urrunetik kodea exekutatzeko bezeroan, PI SQL Client-en erabiltzailearen baimen berdinekin. PI SQL bezeroa ahula izateko beharrezkoa da PI SQL Data Access Server (RTQP Engine) zerbitzari batekiko komunikazioa. Ahultasun horretarako CVE-2019-9765 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Delta Electronics-en TPEditor-en

Argitalpen data: 2019/09/11

Garrantzia: Altua

Kaltetutako baliabideak:

TPEditor, 1.94 eta lehenagoko bertsioak.

Azalpena:

9sg Security Team-eko kimiya ikertzaileak, Trend Micro-ko Zero Day Initiative-rekin (ZDI) batera, bufferraren gainezkatze eta mugez kanpoko irakurketa erako hainbat ahultasunen berri eman dute, Delta Electronics-en TPEditor softwareari eragiten diona. Urruneko erasotzaile batek ahultasun horiek arrakastaz baliatuz gero, informazioa heda lezake, urruneko kodea exekutatu edo aplikazioa geldiarazi.

Konponbidea:

Ahultasuna konpontzeko Delta Electronics-ek 1.95 bertsiora eguneratzea gomendatzen du.

Xehetasuna:

- Pilan (*stack*) oinarritutako bufferraren gainezkatze erako hainbat ahultasun baliatuak izan daitezke bereziki diseinatutako proiektuko fitxategiak prozesatzean. Horiei esker urruneko erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2019-13540 identifikatzailea erreserbatu da.
- Memoria dinamikoan (*heap*) oinarritutako bufferraren gainezkatze erako hainbat ahultasun baliatuak izan daitezke bereziki diseinatutako proiektuko fitxategiak prozesatzean. Horiei esker urruneko erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2019-13536 identifikatzailea erreserbatu da.
- Mugez kanpoko idazketa erako hainbat ahultasun baliatuak izan daitezke bereziki diseinatutako proiektuko fitxategiak prozesatzean. Horiei esker kode arbitrarioa exekuta liteke. Ahultasun horretarako CVE-2019-13544 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Ahultasuna Eaton-en Intelligent Power Protector (IPP) software-n

Argitalpen data: 2019/09/11

Garrantzia: Altua

Kaltetutako baliabideak:

- Intelligent Power Protector, 1.61 eta lehenagoko bertsioak.

Azalpena:

Eaton-ek kritikotasun altuko ahultasun bat aurkitu du Intelligent Power Protector softwarean.

Konponbidea:

Intelligent Power Protector-en 1.66 bertsiora eguneratzea. Kaltetutako produktua erabiltzen duten bezero guztiei gomendatzen zaie bertsio horretara eguneratzea, euren deskargen zentroan eskuragarri.

Xehetasuna:

Erasotzaile batek direktorio jauzi bat egin lezake edo *man-in-the-middle* erako eraso bat egin.

Etiketak: Eguneraketa, Ahultasuna

Bufferraren gainezkatzea Advantech-en WebAcces/SCADAn

Argitalpen data: 2019/09/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Advantech WebAccess/SCADA 8.4.1

Azalpena:

Tenablek bufferraren gainezkatze erako ahultasun bat aurkitu du. Autentifikatu gabeko erasotzaile batek kode arbitrarioa exekuta lezake.

Konponbidea:

8.4.2 bertsiora eta ondorengoetara eguneratzea.

Xehetasuna:

Akatsa *GetUserPasswd* funtzioak dauka, *BwPAlarm.dll* liburutegian dagoena. Bere jatorria da erabiltzaileak emandako datuen baliozkotze okerra, tamaina finkoko bufferrean kopiatu aurretik, RPC IOCTL 70603 mezu bat prozesatzen denean.Autentifikatu gabeko erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2019-3975 identifikatzailea erabili da.

Etiketak: Eguneraketa, SCADA, Ahultasuna

Ahultasuna Philips-en IntelliVue WLANen

Argitalpen data: 2019/09/12

Garrantzia: Ertaina

Kaltetutako baliabideak:

IntelliVue WLAN modulua (Wireless Local Area Network), A eta B bertsioak.

Azalpena:

Philips-ek IntelliVue Patient Monitors ekipoek erabiltzen duten IntelliVue WLAN moduluari eragiten dion ahultasun bat aurkitu du, A eta B bertsioetan.

Konponbidea:

Philipsek kaltetutako moduluak C bertsioarekin ordezkatzea gomendatzen du, orain duten *firmware* bertsioari (B.00.31) ez baitio eragiten ahultasun horrek. A bertsioari dagokionez, Philipsek dio 2019. urtearen amaieran ahultasun hori konpontzen duen partxe bat argitaratuko duela.B bertsioak ez dauka jarraipenik.

Xehetasuna:

Baimenik gabeko erabiltzaile batek, ezagutza handiak balitu eta gailuaren sare lokalera sarbidea balu, gailuaren *firmwarea* eta datuen fluxua kaltetu litzake.

Etiketak: Eguneraketa, Osasuna, Ahultasuna

Hainbat ahultasun 3S-Smart Software Solutions GmbHren CODESYS produktuetan

Argitalpen data: 2019/09/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Ondorengo CODESYS V3 produktuen aldaera guztiak, 3.5.14.10 baino lehenagoko bertsio guztietan web zerbitzaria baldin badute (CmpWebServer):
  - BeagleBone-rako CODESYS Control;
  - emPC-A/iMX6rako CODESYS Control;
  - IOT2000erako CODESYS Control;
  - Linuxerako CODESYS Control;
  - PFC100erako CODESYS Control;
  - PFC200erako CODESYS Control;
  - Raspberry Pi-rako CODESYS Control;
  - RTE V3rako CODESYS Control;
  - CODESYS Control RTE V3 (Beckhoff CXerako);
  - CODESYS Control Win V3 (CODESYS Development System-en konfigurazioaren zati bat ere bai);
  - CODESYS HMI V3;
  - CODESYS Control V3 Runtime System Toolkit;
  - CODESYS V3 Embedded Target Visu Toolkit;
  - CODESYS V3 Remote Target Visu Toolkit.
- Ondorengo CODESYS Control V3 produktuen aldaera guztiak, 3.5.11.0tik 3.5.15.0ra bitarteko bertsio guztietan, OPC UA Security erabiltzen duen CODESYSen OPC UA zerbitzaria baldin badute:
  - BeagleBone-rako CODESYS Control;
  - emPC-A/iMX6rako CODESYS Control;
  - OT2000erako CODESYS Control;
  - Linuxerako CODESYS Control;
  - PFC200erako CODESYS Control;
  - Raspberry Pi-rako CODESYS Control;
  - RTE V3rako CODESYS Control;
  - CODESYS Control RTE V3 (Beckhoff CXerako);
  - CODESYS Control Win V3 (CODESYS Development System-en konfigurazioaren zati bat ere bai);
  - CODESYS Control V3 Runtime System Toolkit.
- CODESYS Development System V3, 32 eta 64 bit-eko arkitekturetan, 3.5.15.0 baino lehenagoko bertsioak.
- CODESYS V2.3 ENI zerbitzariak, 3.2.2.24 baino lehenagoko bertsioak.

Azalpena:

3S-Smart Software Solutions GmbHren CODESYS produktu batzuetan aurkitutako hainbat ahultasunen berri eman da. Ahultasun horiek arrakastaz baliatuz gero, erasotzaile batek zerbitzuaren ukapen egoera sor lezake, urrunetik kodea exekutatu, manipulatutako liburutegietako asmo gaiztoko edukia exekutatu edo erakutsi, edo fitxategi murriztuetara sarbidea lortu.

Konponbidea:

Ahultasun horiek konpontzeko ekipoak softwarearen ondorengo bertsioetara eguneratzea gomendatzen da:

- 3.2.2.24;
- 3.5.12.80;
- 3.5.14.10;
- 3.5.15.0.

Xehetasuna:

- Bereziki diseinatutako http edo https eskari bat baliatuz, erasotzaile batek kontrolatzailearen lan direktoriotik kanpoko fitxategietara sarbidea lor lezake. Ahultasun horretarako CVE-2019-13532 identifikatzailea erreserbatu da.
- Bereziki diseinatutako http edo https eskari batek bufferraren gainezkatzea eragin lezake, eta horren ondorioz zerbitzuaren ukapen egoera sor liteke edo kodea exekutatu urrunetik. Ahultasun horretarako CVE-2019-13548 identifikatzailea erreserbatu da.
- Sistemak aktibo dagoen liburutegiaren edukia erakusten du bere baliagarritasuna egiaztatu gabe. Horrek liburutegi manipulatuak exekutatzea edo horien edukia erakustea ahalbidetu lezake. Ahultasun horretarako CVE-2019-13538 identifikatzailea erreserbatu da.
- Konfiantzazko OPC UA bezero baten bereziki diseinatutako eskaera batek NULL erakusle baten deserreferentzia eragin lezake, eta horren ondorioz zerbitzuaren ukapen egoera gerta liteke. Ahultasun horretarako CVE-2019-13542 identifikatzailea erreserbatu da.
- Bereziki diseinatutako eskaera batek pilan oinarritutako bufferraren gainezkatzea eragin lezake, eta ondorioz kode arbitrarioa exekuta liteke ENI zerbitzarian, edo zerbitzuaren ukapen egoera eragin liteke, zerbitzari horren akats bat dela eta.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Hainbat ahultasun Bosch-en Access Professional Edition-en

Argitalpen data: 2019/09/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Bosch Access Professional Edition (APE), 3.7 eta lehenagoko bertsioak.

Azalpena:

Oleksii Orekhov ikertzaile independenteak, Bosch-ekin koordinaturik, bi ahultasun aurkitu ditu, bat larritasun kritikokoa eta bestea altukoa. Erasotzaile batek informazio konfidentziala heda lezake edo administratzaile pribilegioak eskuratu.

Konponbidea:

APE 3.8 bertsiora edo goragoko batera eguneratzea.

Xehetasuna:

- APE zerbitzariaren sarera sarbidea lukeen autentifikatu gabeko erasotzaile batek informazio konfidentziala ezagutzera eman lezake edo administrazio pribilegioak lortu, alderantzizko ingeniaritzaren bidez. Ahultasun horretarako CVE-2019-11898 identifikatzailea

erabili da.
- APE zerbitzariaren sarera sarbidea lukeen autentifikatu gabeko erasotzaile batek bezeroan informazio konfidentziala eskura lezake SMB protokoloaren bidez. Ahultasun horretarako CVE-2019-11899 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Informazioa agerian uztea Siemens-en SINEMA Remote Connect Server-en

Argitalpen data: 2019/09/18

Garrantzia: Ertaina

Kaltetutako baliabideak:

SINEMA Remote Connect Server, 2.0 SP1 baino lehenagoko bertsioak.

Azalpena:

HOWEST-eko Hendrik Derre eta Tijl Deneut ikertzaileek informazioa agerian uzte erako ahultasun baten berri eman dute. Hori baliatuz baimenik gabeko erasotzaile batek erabiltzailearen eta gailuaren informazio pribilegiatura sarbidea lor lezake.

Konponbidea:

Siemens-ek SINEMA Remote Connect Server 2.0 SP1 bertsiora edo geroagoko batera eguneratzea gomendatzen du.

Xehetasuna:

Soilik erabiltzaile pribilegiatu bat sar litekeen orrialde batzuetara sarbidea lor lezake erabiltzaile pribilegiatua ez den batek ere. Sarera sarbidea lukeen eta web interfazerako kredentzial baliagarriak lituzkeen erabiltzaile batek informazio pribilegiatua ezagutzera eman lezake. Informazio horien artean ez dago pasahitzik. Ahultasun horretarako CVE-2019-34623 identifikatzailea erabili da.

Etiketak: Eguneraketa, Siemens, Ahultasuna

Informazioa agerian uztea Honeywell-en Performance IP Cameras eta Performance NVRs-en

Argitalpen data: 2019/09/18

Garrantzia: Ertaina

Kaltetutako baliabideak:

- Performance IP Cameras:
  - HBD3PR2;
  - H4D3PRV3;
  - HED3PR3;
  - H4D3PRV2;
  - HBD3PR1;
  - H4W8PR2;
  - HBW8PR2;
  - H2W2PC1M;
  - H2W4PER3;
  - H2W2PER3;
  - HEW2PER3;
  - HEW4PER3B;
  - HBW2PER1;
  - HEW4PER2;
  - HEW4PER2B;
  - HEW2PER2;
  - H4W2PER2;
  - HBW2PER2;
  - H4W2PER3;
  - HPW2P1.
- Performance NVRs:
  - HEN08104;
  - HEN08144;
  - HEN081124;
  - HEN16104;
  - HEN16144;
  - HEN16184;
  - HEN16204;
  - HEN162244;
  - HEN16284;
  - HEN16304;
  - HEN16384;
  - HEN32104;
  - HEN321124;
  - HEN32204;
  - HEN32284;
  - HEN322164;
  - HEN32304;
  - HEN32384;
  - HEN323164;

- HEN64204;
- HEN64304;
- HEN643164;
- HEN643324;
- HEN643484;
- HEN04103;
- HEN04113;
- HEN04123;
- HEN08103;
- HEN08113;
- HEN08123;
- HEN08143;
- HEN16103;
- HEN16123;
- HEN16143;
- HEN16163;
- HEN04103L;
- HEN08103L;
- HEN16103L;
- HEN32103L.

Azalpena:

Ismail Bulbil ikertzaile independenteak informazioaren agerpen erako ahultasun baten berri eman du. Hori baliatuz erasotzaile batek kaltetutako gailuaren konfigurazioari buruzko informazioa eskura lezake.

Konponbidea:

Honeywell-ek kaltetutako produktu guztietarako firmware eguneraketak argitaratu ditu. Bere webgunean eskura daitezke.

Xehetasuna:

Kaltetutako gailuen web zerbitzari barneratua baliatuz, urruneko erasotzaile batek web konfigurazioaren datuak eskura litzake, JSON formatuan, IP eta NVRs (Network Video Recorders) kameren kasuan, horietara sarearen bidez sarbidea lor baitaiteke autentifikatu behar izan gabe. Ahultasun horretarako CVE-2019-13523 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Hainbat ahultasun Advantech-en WebAccess-en

Argitalpen data: 2019/09/18

Garrantzia: Kritikoa

Kaltetutako baliabideak:

WebAccess, 8.4.1 eta lehenagoko bertsioak.

Azalpena:

Elextec Security Tech. Co. Ltd.-eko Peter Cheng-ek eta Trend Micro's Zero Day Initiative-ko Mat Powell-ek, VenusTech-eko ADLab-ekin batera, hainbat eratako ahultasunak aurkitu dituzte: kodearen injekzioa, komandoen injekzioa, eta bufferraren pilaren gainezkatzea eta baimentze desegokia. Horiek baliatuz erasotzaile batek kode arbitrarioa exekuta lezake, fitxategietara sarbidea lortu, eta ekintzak exekutatu pribilegio maila altu batekin, edo sisteman fitxategiak ezabatu.

Konponbidea:

Azaldutako ahultasunak konpontzeko Advantech-ek WebAccessNode-ren 8.4.2 bertsioa argitaratu du.

Xehetasuna:

- Sarean *exploit* bat exekutatzeak kodea sortzean kontrol oker bat eragin lezake. Horren ondorioz urrunetik kodea exekuta liteke, datuak exfiltratu edo sistemaren blokeatzea eragin. Ahultasun horretarako CVE-2019-13558 identifikatzailea erreserbatu da.
- Komandoen injekzio erako hainbat ahultasun gertatzen dira erabiltzaileak emandako datuak baliozkotzen ez direlako. Horrek fitxategien ezabatze arbitrarioa eragin lezake eta kodea urrunetik exekutatzea. Ahultasun horretarako CVE-2019-13552 identifikatzailea erreserbatu da.
- Pilan oinarritutako bufferraren gainezkatze erako hainbat ahultasun daude, erabiltzaileak emandako datuen luzeraren baliozkotze egoki baten faltak eraginda. Hori baliatuz erasotzaile batek urruneko kodea exekuta lezake. Ahultasun horretarako CVE-2019-13556 identifikatzailea erreserbatu da.
- Baimentze desegoki erako ahultasun bat baliatuz erasotzaile batek informazio sentikorra ezagutzera eman lezake eta kodea sortzearen kontrol desegokia eragin. Ondorioz urruneko kodea exekuta liteke edo sistemaren blokeatzea eragin. Ahultasun horretarako CVE-2019-13550 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Dräger-en produktuetan

Argitalpen data: 2019/09/19

Garrantzia: Altua

Kaltetutako baliabideak:

- Dräger Infinity Acute Care System, VG4.1.1/VG4.0.3 eta lehenagoko bertsioak.
- Dräger Standalone Infinity M540, VG4.1.1 eta lehenagoko bertsioak.

Azalpena:

Ahultasun batzuk aurkitu dira Dräger-en hainbat produktutan, datuen faltsutze eta manipulatze, eta banatutako zerbitzuaren ukapen erakoak. Ahultasun horiek gailua berrabiaraztea edo funtzionaltasuna galtzea eragin lezakete.

Konponbidea:

Dräger-ek gailuen softwarea eguneratzea gomendatzen du:

- Infinity Acute Care System, VG4.1.2/VG4.0.3 edo geroagoko bertsioa.
- Standalone Infinity M540, VG4.1.2 edo geroagoko bertsioa.

Xehetasuna:

- Gailuek bidalitako datuak faltsutuak edo manipulatuak izan daitezke, eta horrek datuak monitorizatzeko sareei eta nodoei eragingo lioke. Era berean, gailuetara bidalitako datuak ere faltsutu litezke. Ondorioz, gailuaren konfigurazio batzuk alda litezke urrunetik, gailuak berak urruneko kontrola onartzen badu Infinity Central Station-en (ICS) bidez.
- Zerbitzuaren ukapen erako ahultasun bat dago, aplikazioaren sarrera paketeen tamaina eta kopuruaren kudeaketa oker batek eraginda. Horrek gailuak berrabiaraztea eta saretik deskonektatzea eragin lezake. Ahultasun hau baliatzeko erasotzaileak sarbide fisikoa izan beharra dauka gailuen sarera dedikatutako ataka batetara. Eraso hau gerta daiteke gailua haririk gabeko sare batera konektatzen denean ere, eta horrek bere berrabiatzea eragingo luke. Nolanahi ere, haririk gabeko konfigurazioa soilik dago aktibo gailua garraioan dagoenean.

Etiketak: Eguneraketa, Osasuna, Ahultasuna

Informazioaren agerpenak WAGOren PFC100/PFC200 kontrolatzaileetan

Argitalpen data: 2019/09/19

Garrantzia: Ertaina

Kaltetutako baliabideak:

- 12. bertsioa baino lehenagoko firmwarea duten PFC100 eta PFC200 serieetako kontrolatzaileak.

Azalpena:

Fachhochschule Aachen-eko Nico Jansen ikertzaileak kritikotasun ertaineko ahultasun baten berri eman du, WAGOren produktuei eragiten diena. Urruneko erasotzaile batek instalatutako softwarea identifika lezake, edo informazio sentikorra ezagutzera eman.

Konponbidea:

Gailuen firmwarea 12. bertsiora edo berriago batera eguneratzea.

Xehetasuna:

Ahultasunaren jatorria da fitxategien existentzia egiaztatzeko bereziki sortzen diren HTTP eskaerak bidaltzeko aukera. Urruneko erasotzaile batek instalatutako softwarea identifika lezake, edo informazio sentikorra ezagutzera eman.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Tridium-en Niagara produktuetan

Argitalpen data: 2019/09/20

Garrantzia: Altua

Kaltetutako baliabideak:

- Niagara AX 3.8u4 (JACE 3e, JACE 6e, JACE 7, JACE-8000);
- Niagara 4.4u3 (JACE 3e, JACE 6e, JACE 7, JACE-8000);
- Niagara 4.7u1 (JACE-8000, Edge 10).

Azalpena:

Secure Mobile Networking Lab-eko Johannes Eger eta Fabian Ullrich ikertzaileek bi ahultasunen berri eman dute. Bata larritasun altukoa da, eta bestea ertainekoa, informazioaren agerpen eta baimentze desegoki erakoak, hurrenez hurren. Horiek baliatuz erasotzaile lokal batek bere pribilegioak eskalatzea lor lezake.

Konponbidea:

Ahultasun horiek konpontzeko Tridium-ek ondoren aipatzen diren eguneraketak argitaratu ditu. Salmenta zerbitzuko kanalarekin edo Tridium-en zerbitzu ekipoarekin harremanetan jarriz eskura daitezke:

- Niagara AX 3.8u4:
  - OS Dist: 2.7.402.2;
  - NRE Config Dist: 3.8.401.1.
- Niagara 4.4u3:
  - OS Dist: 4.4.73.38.1 NRE Config;
  - Dist: 4.4.94.14.1.
- Niagara 4.7u1:
  - OS Dist: (JACE 8000) 4.7.109.16.1;
  - OS Dist (Edge 10): 4.7.109.18.1;
  - NRE Config Dist: 4.7.110.32.1.

Xehetasuna:

- *QNX* *procfs* zerbitzuak prozesu eta baliabideei buruzko informaziorako sarbidea ematen du. Hori baliatuz pribilegio maila baxuagoko prozesu batek xede den helbideen espaziora sarbidea lor lezake. Ahultasun horretarako CVE-2019-8998 identifikatzailea erabili da.
- Utilitate jakin bat baliatuz erasotzaile batek pribilegioak dituzten fitxategiak irakurtzeko sarbidea lor lezake. Ahultasun horretarako CVE-2019-13528 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IoT, Ahultasuna

Hainbat ahultasun Moxa produktuetan

Argitalpen data: 2019/09/25

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- PT-7528 Series, 4.0 bertsioa eta lehenagokoak.
- PT-7828 Series, 3.9 bertsioa eta lehenagokoak.
- ioLogik 2500 Series, 3.0 bertsioa eta lehenagokoak.
- IOxpress Configuration Utility, 2.3.0 bertsioa eta lehenagokoak.
- MB3170 Series, 4.0 bertsioa eta lehenagokoak.
- MB3270 Series, 4.0 bertsioa eta lehenagokoak.
- MB3180 Series, 2.0 bertsioa eta lehenagokoak.
- MB3280 Series, 3.0 bertsioa eta lehenagokoak.
- MB3480 Series, 3.0 bertsioa eta lehenagokoak.
- MB3660 Series, 2.2 bertsioa eta lehenagokoak.
- EDS-G516E Series, 5.2 bertsioa eta lehenagokoak.
- EDS-510E Series, 5.2 bertsioa eta lehenagokoak.

Azalpena:

Rostelecom-Solar-eko Ilya Karpov eta Evgeniy Druzhinin ikertzaileek, Positive Technologies-eko Georgy Zaytsev eta Maxim Kozhevnikov-ekin batera, Moxaren hainbat produkturi eragiten dieten ahultasun batzuen berri eman dute.

Konponbidea:

Moxak eguneraketa ezberdinak garatu ditu kaltetutako gailuentzat, eta euren zerbitzu teknikoaren zentroan eskura daitezke.

Xehetasuna:

Aurkitutako ahultasun motak honako hauek dira:

- Pilan oinarritutako bufferraren gainezkatzea.
- Segurua ez den algoritmo kriptografikoaren erabilpena.
- Kodetutako gako kriptografiko baten erabilpena.
- Kodetutako pasahitz baten erabilpena.
- Pasahitz ahulen eskakizunak.
- Informazioaren agerpena.
- Algoritmo kriptografiko ahulen erabilpena.
- Testu lauan gordetzea eta informazio konfidentziala transmititzea.
- Zerbitzuaren ukapena.
- Osoko zenbakiaren gainezkatzeak bufferraren gainezkatzea eragitea.
- CSRF (*Cross-site request forgery*).
- Bufferra kopiatzea sarreraren tamaina egiaztatu gabe.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Sarreren baliozkotze okerra Yokogawa-ren hainbat gailutan

Argitalpen data: 2019/09/27

Garrantzia: Altua

Kaltetutako baliabideak:

- Exaopc, R1.01.00 bertsiotik R3.77.00 bertsioa bitartekoak;
- Exaplog, R1.10.00 bertsiotik R3.40.00 bertsiora bitartekoak;
- Exaquantum, R1.10.00 bertsiotik R3.02.00 bertsiora bitartekoak;
- Exaquantum/Batch, R1.01.00 bertsiotik R2.50.40 bertsiora bitartekoak;
- Exasmoc, bertsio guztiak;
- Exarge, bertsio guztiak;
- GA10, R1.01.01 bertsiotik R3.05.01 bertsioa bitartekoak;
- InsightSuiteAE, R1.01.00 bertsiotik R1.06.00 bertsiora bitartekoak.

Azalpena:

Yokogawa-ko ekipoak sarreren baliozkotze oker erako ahultasunaren berri eman du. Hori baliatuz, erasotzaile lokal batek asmo gaiztoko fitxategiak exekuta litzake zerbitzuaren pribilegioaren bidez.

Ebazpena:

- Exaopc: R3.78.00 bertsiora eguneratzea;
- Exaplog: R3.40.00 bertsiora eguneratzea eta R3.40.06rako partxea aplikatzea;

- Exaquantum: R3.15.00 bertsiora eguneratzea;
- Exaquantum/Batch: R3.10.00 bertsiora eguneratzea;
- Exasmoc: 2019ko irailaren 30ean amaitzen zaio zerbitzua, eta horregatik Exasmoc-en jarraitzailea den *Platform for Advanced Control and Estimation*-era migratzea gomendatzen da;
- Exarqe: 2019ko irailaren 30ean amaitzen zaio zerbitzua, eta horregatik Exarqe-ren jarraitzailea den *Platform for Advanced Control and Estimation*-era migratzea gomendatzen da;
- GA10: R3.05.06 bertsiora eguneratzea;
- InsightSuiteAE: R1.07.00 bertsiora eguneratzea.

Xehetasuna:

Yokogawa-ren aplikazio batzuetan zerbitzuen bidea ez dago komatxoen artean idatzita eta zuriuneak ditu. Hori baliatuz erasotzaile lokal batek asmo gaiztoko fitxategi bat exekuta lezake zerbitzuaren pribilegioaren bidez.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Moxa-ren EDR-810 serieko routerretan

Argitalpen data: 2019/09/30

Garrantzia: Altua

Kaltetutako baliabideak:

EDR-810 serieko routerrak, 5.1 eta lehenagoko bertsioak.

Azalpena:

Guillaume Lopes de Randorisec ikertzaileak kritikotasun altuko bi ahultasunen berri eman du. Erasotzaile batek baimendu gabeko komandoak exekuta litzake routerrean eta *log*-eko informazioa eskuratu.

Konponbidea:

5.3 bertsiora edo berriagora eguneratzea.

Xehetasuna:

- Baimenik gabeko erasotzaile batek komandoak exekuta litzake routerrean, web kontsolako Admin eta ConfigAdmin kontuen baliozkotze okerra dela eta. Ahultasun horretarako CVE-2019-10969 identifikatzailea erreserbatu da.
- Autentifikaziorik gabeko erasotzaile batek log-aren bidez eskuratutako informazio sentikorra agerian utz lezake. Ahultasun horretarako CVE-2019-10963 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna