2019ko Maiatzaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Hainbat ahultasun GEren komunikatzaileetan

Argitalpen data: 2019/05/03

Garrantzia: Handia

Kaltetutako baliabideak:

- Communicator Installer, Application, PostGreSQL, MeterManager eta WISE Uninstaller, 4.0.517 baino lehenagoko bertsioak.

Azalpena:

Dragos-eko Reid Wightman ikertzaileak hainbat ahultasunen berri eman du, era hauetakoak: kontrolatu gabeko bilaketa bidea, barneratutako kredentzialen erabilpena eta sarbide kontrol okerra. Erasotzaile batek administratzaile baimenak eskura litzake, widgetak eta erabiltzaile interfazeak manipulatu, datu basearen kontrola eskuratu edo administraziorako erreserbatutako komandoak exekutatu.

Konponbidea:

- Fabrikatzaileak gomendatzen du komunikatzaileak 4.0.517 edo goragoko bertsiora eguneratzea.

Xehetasuna:

- Administrazio baimenik gabeko erasotzaile batek asmo gaiztoko fitxategiak koka litzake instalatzailearen fitxategi direktorioan, sistema batean administratzaile pribilegioak eskuratzeko asmoz instalazioan edo eguneraketan zehar. Ahultasun horretarako CVE-2019-6564 identifikatzailea erreserbatu da.
- Erasotzaile batek asmo gaiztoko fitxategiak koka litzake programaren lan direktorioan, widgetak eta erabiltzailearen interfazearen elementuak manipulatzeko asmoz. Ahultasun horretarako CVE-2019-6546 identifikatzailea erreserbatu da.
- Backdoor izaera duten bi erabiltzaile kontu daude, eta haiek baliatuz erasotzaile batek datu basearen kontrola lor lezake. Erasotzaileak zerbitzu horretarako sarbidea ezin du lortu baldin eta biktimak Windowsen suebakiaren konfigurazio lehenetsia erabiltzen badu. Ahultasun horretarako CVE-2019-6548 identifikatzailea erreserbatu da.
- Sistemaren baimenekin exekutatutako zerbitzu bat baliatuz, baimenik gabeko erasotzaile batek hainbat ekintza administratibo egin litzake. Horren ondorioz sisteman script programatuak exekuta litzake administratzaile pribilegioekin. Erasotzaileak zerbitzu horretarako sarbidea ezin du lortu baldin eta biktimak Windowsen suebakiaren konfigurazio lehenetsia erabiltzen badu. Ahultasun horretarako CVE-2019-6544 identifikatzailea erreserbatu da.
- Administrazio baimenik gabeko erasotzaile batek desinstalatzailea ordezka dezake asmo gaiztoko bertsio batekin, eta horrela sisteman administratzaile pribilegioak lortu. Ahultasun horretarako CVE-2019-6566 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Orpak-en SiteOmat-en

Argitalpen data: 2019/05/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SiteOmat, 6.4.414.122 baino lehenagoko bertsioak
- SiteOmat, 6.4.414.084 baino lehenagoko bertsioak

Azalpena:

Kaspersky Lab-eko Ido Naor ikertzaileak era ezberdineko hainbat ahultasunen berri eman du: pasahitz barneratuen erabilpena, Cross-Site Scripting (XSS), SQL injekzioa, datu sentikorretan zifratze falta, kodearen injekzioa eta bufferraren gainezkatzea. Ahultasun horiek arrakastaz baliatuz gero, erasotzaile batek urruneko kodea exekuta lezake zerbitzuaren ukapen egoera eta baimenik gabeko sarbidea

eraginez, monitorizazio, konfigurazio eta ordainketa informazioa ikusi eta editatzeko.

Konponbidea:

- Fabrikatzaileak gomendatzen du kaltetutako bertsioak v6.4.414.139 bertsiora edo berriagora eguneratzea. Eguneraketa eskura daiteke fabrikatzailearekin kontaktatuz Orpak-en laguntza orrialdean (beharrezkoa da erregistratzea).

Xehetasuna:

- Pasahitz barneratuen erabilpena: aplikazioak kredentzial barneratuak erabiltzen ditu. Ahultasun horretarako CVE-2017-14728 identifikatzailea erreserbatu da.
- *Cross-Site Scripting (XSS):* Web aplikazioak ez ditu ondo iragazten sarbide parametroak, eta horren ondorioz *Cross-Site Scripting-a* balia daiteke. Ahultasun horretarako CVE-2017-14850 identifikatzailea erabili da.
- SQL injekzioa: aplikazioak ez ditu modu egokian iragazten sarrera parametroak. Horren ondorioz, erasotzaile bat produktuaren informaziora sarbidea lor lezake bereziki diseinatutako sarrera bat sartuz. Ahultasun horretarako CVE-2017-14851 identifikatzailea erreserbatu da.
- Datu sentikorren zifratze falta: aplikazioak informazio sentikorra bidaltzen du testu lauan. Bidalitako informazio sentikorraren artean kredentzialak daude. Erasotzaile batek saretik bidalitako kredentzialak atzeman litzake eta kaltetutako produktuaren autentifikazioari ihes egin. Ahultasun horretarako CVE-2017-14852 identifikatzailea erreserbatu da.
- Kodearen injekzioa: aplikazioak ez ditu modu egokian murrizten kanpoko sarrera parametroak. Horren ondorioz autentifikatu gabeko erasotzaile batek bereziki diseinatutako kodea exekuta lezake biktima den sisteman. Ahultasun horretarako CVE-2017-14853 identifikatzailea erreserbatu da.
- Bufferrak gainezka egitea: aplikazioak erabiltzen duen funtzio batek erabiltzaileen sarrera parametroak onartzen ditu. Sarrera horrek ez du trataera zuzen bat, eta ondorioz erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2017-14854 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna

Hainbat ahultasun Sierra Wireless-en AirLink ALEOSen

Argitalpen data: 2019/05/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- LS300, GX400, GX440 eta ES440, 4.4.8 eta lehenagoko bertsioak.
- GX450 y ES450, 4.9.4 baino lehenagoko bertsioak.
- MP70, MP70E, RV50, RV50X, LX40 eta LX60, 4.12 baino lehenagoko bertsioak.

Azalpena:

Cisco Talos-eko Carl Hud eta Jared Rittle ikertzaileek Sierra Wireless-en AirLink ALEOS produktuei eragiten dieten hainbat ahultasun aurkitu dituzte, era ezberdinetakoak: Sistema Eragileko komandoen injekzioa, barneratutako kredentzialen erabilpena, fitxategi arriskutsuen igoera ez murriztua, cross-site scripting (XSS), cross-site request forgery (CSRF), informazioa agerian uztea, datu sentikorren enkriptatze falta, pasahitzaren aldaketa ez egiaztatua eta baliabide kritikoetarako baimenen esleipen okerra. Ahultasun horiek arrakastaz baliatuz gero, erasotzaile batek urruneko kodea exekuta lezake, erabiltzailearen kredentzialak zein diren asmatu, fitxategiak igo edo fitxategi bideak aurkitu.

Konponbidea:

Fabrikatzaileak gomendatzen du ALEOSen azken bertsioetara eguneratzea ondoren aipatzen diren produktu eta bertsioen kasuan (horietako batzuk oraindik ez daude eskuragarri):

- LS300, GX400, GX440, ES440: ALEOS 4.4.9 (2019 amaieran eskuragarri).
- GX450, ES450: ALEOS 4.9.4.p09 (dagoeneko eskuragarri).
- MP70, MP70E, RV50, RV50X, LX40, LX60: ALEOS 4.12 (2019ko ekainaren amaieran eskuragarri).

Aurrekoaz gain, Sierra Wireless-ek honako jarraibide hauek ere gomendatzen ditu:

- Pasahitz sendoa erabiltzen dela ziurtatzea.
- ALEOS Application Framework (AAF) aktibatuta badago, AAF erabiltzailearen kontuan pasahitz sendoa erabiltzen dela ziurtatzea.
- Telnet edo SSH erabiltzen bada, kontsolaren kontuan pasahitz sendoa erabiltzen dela ziurtatzea.
- ACEmanager-era zuzenean konektatzean:
  - HTTPS soilik erabiltzea.
  - Nabigatzaile moderno eta eguneratu bat erabiltzea, esate baterako Chrome, Firefox edo Edge.

Xehetasuna:

- Autentifikatutako HTTP eskaera batek, bereziki diseinatuta badago, komando arbitrarioak injekta ditzake eta ondorioz kodea urrunetik exekutatu. Ahultasun horretarako CVE-2018-4061 identifikatzailea erreserbatu da.
- WebUItik kanpo SNMPD aktibatzeak kodifikatutako kredentzialak aktibatzea eragingo luke eta ondorioz erabiltzaile pribilegiatu bat agerian geldituko litzateke. Ahultasun hori baliatzeko erasotzaile batek SNMPD aktiba dezake, konfigurazioaren inolako aldaketarik gabe.
- Autentifikatutako HTTP eskaera batek, bereziki diseinatuta badago, fitxategi bat karga dezake, eta ondorioz exekutagarria eta web zerbitzarira bideragarria den kodea kargatuko luke. Ahultasun horretarako CVE-2018-4063 identifikatzailea erreserbatu da.
- Bereziki diseinatutako HTTP eskari batek konfigurazio aldaketa eragin dezake egiaztatu gabeko gailu batean. Ondorioz, erabiltzailearen pasahitzaren egiaztatu gabeko aldaketa gertatuko litzateke gailuan. Erasotzaile batek autentifikatutako HTTP eskari bat egin dezake ahultasun hori baliatzeko. Ahultasun horretarako CVE-2018-4064 identifikatzailea erreserbatu da.
- Bereziki diseinatutako ping HTTP eskari batek JavaScript islatua erabiltzailearen nabigatzailean exekutatzea eragin dezake. Erasotzaile batek ahultasun hori balia dezake erabiltzaile bat engainatuz lotura batean edo txertatutako URL batean klik egin dezan, eta horrela webguneen arteko komandoen sekuentzien ahultasun islatura birbideratuko luke. Ahultasun horretarako CVE-2018-4065 identifikatzailea erreserbatu da.
- Bereziki diseinatutako HTTP eskari batek eragin dezake autentifikatutako erabiltzaile batek eskari pribilegiatuak egitea jakin gabe, eta ondorioz autentifikatu gabeko eskaerak sortuko lirateke erabiltzaile horren bidez. Ahultasun hori gertatuz gero erasotzaile bat autentifikatutako orrialdeetara sartuko litzateke identifikatutako erabiltzaile baten bidez. Ahultasun horretarako CVE-2018-4066 identifikatzailea erreserbatu da.
- Autentifikatutako HTTP eskari batek, bereziki diseinatuta badago, informazioaren ihesa eragin lezake, eta ondorioz fitxategien barne bideak agerian geldituko lirateke. Ahultasun horretarako CVE-2018-4067 identifikatzailea erreserbatu da.

- HTTP eskari batek gailuaren konfigurazio lehenetsia agerian utz dezake. Erasotzaile batek autentifikatu gabeko HTTP eskari bat egin dezake ahultasun hori baliatzeko. Ahultasun horretarako CVE-2018-4068 identifikatzailea erreserbatu da.
- ACEManager-en autentifikazio funtzionaltasuna XML testu lauan egiten da web zerbitzarira. Erasotzaile batek gailutik sareko trafikoa entzun dezake ahultasun hori baliatzeko. Ahultasun horretarako CVE-2018-4069 identifikatzailea erreserbatu da.
- Bereziki diseinatutako HTTP eskari batek informazioa agerian uztea eragin dezake, eta ondorioz informazio konfidentziala agerian geldituko litzateke, testu lauko pasahitzak eta SNMP kateak barne, baina ez horiek soilik. Ahultasun hori baliatzeko erasotzaile batek autentifikatutako HTTP eskari bat egin dezake edo bitarra exekutatu. Ahultasun horretarako CVE-2018-4070 eta CVE-2018-4071 identifikatzaileak erreserbatu dira.
- Bereziki diseinatutako HTTP eskari batek konfigurazio arbitrario bat idaztea eragin dezake, eta ondorioz sistemaren edozein konfiguraziotan aldaketa ez egiaztatuak gertatuko lirateke. Ahultasun hori baliatzeko erasotzaile batek autentifikatutako HTTP eskari bat egin dezake, edo edozein erabiltzaileren modura bitarra exekutatu. Ahultasun horretarako CVE-2018-4072 eta CVE-2018-4073 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Sarbideen kontrol desegokia Bosch-en Video Recording Manager-en

Argitalpen data: 2019/05/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Bosch Diver IP 5000, 3.80.0033, 3.80.0035 eta 3.80.0037 bertsioak.
- Bosch Video Recording Manager, 3.70.0056, 3.70.0058, 3.70.0060, 3.70.0062, 3.71.0022, 3.71.0029, 3.71.0031, 3.71.0032, 3.81.0032, 3.81.0038 eta 3.81.0048 bertsioak.
-
- Bosch Video Management System, 7.5 eta 8.0 bertsioak, VRMren ondorengo bertsio ahulak erabiltzen dituztenak: 3.70.0056, 3.70.0058, 3.70.0060, 3.70.0062, 3.71.0022, 3.71.0029, 3.71.0031, 3.71.0032.
- Bosch Video Management System, 9.0 bertsioa, VRMren honako bertsio ahul hauek erabiltzen dituena: 3.81.0032, 3.81.0038, 3.81.0048.

Azalpena:

Bosch-ek sarbideen kontrol desegoki erako ahultasun baten berri eman du, bere Video Recording Manager (VRM) softwareari eragiten diona. Hori baliatuz, autentifikaziorik gabeko urruneko erasotzaile batek sarbidea lor lezake ziurtagirien azpimultzo mugatu batera.

Konponbidea:

Bere produktuen kasuan Bosch-ek honako hau gomendatzen du:

- DIVAR IP 5000 3.80ren kasuan, 3.80.0039 firmware bertsiora eguneratzea
- Video Recording Manager-en kasuan:
  - 3.70 bertsioaren kasuan, 3.71.0034 bertsiora eguneratzea.
  - 3.71 bertsioaren kasuan, 3.71.0034 bertsiora eguneratzea.
  - 3.81 bertsioaren kasuan, 3.81.0050 bertsiora eguneratzea.
- Bosch Video Management System-en kasuan:
  - 7.5 eta 8.0 bertsioen kasuan, VRM 3.71.0034 bertsiora eguneratzea.
  -
  - 9.0 bertsioaren kasuan, VRMren 3.81.0050 bertsiora eguneratzea.

Xehetasuna:

-
- Sarbideen kontrol desegoki erako ahultasun bat dauka Bosch-en Video Recording Manager softwareak. Hori baliatuz, autentifikaziorik gabeko urruneko erasotzaile batek sarbidea lor lezake sistema eragilean gordetako ziurtagirien azpimultzo batera. Ahultasun horretarako CVE-2019-11684 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Múltiples vulnerabilidades en productos Siemens

Argitalpen data: 2019/05/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

-
- LOGO! Soft Comfort eta BM, bertsio guztiak.
- SCALANCE W1750D, V8.4.0.1 bertsioa baino lehenagoko guztiak.
- NXG I eta NXG II control-dun SINAMICS PERFECT HARMONY GH180, MLFB: 6SR2. . . -, 6SR3. . . -, 6SR4. . .-, G28 aukera duten bertsio guztiak.
- SIMATIC PCS 7 V9.0, V8.2, V8.2 eta V8.0 bertsioak eta lehenagoko bertsio guztiak.
- SIMATIC WinCC (TIA Portal) V15, V14 eta V13, bertsio guztiak.
- SIMATIC WinCC Runtime Professional, bertsio guztiak.
- SIMATIC WinCC V7.2 eta lehenagokoak, bertsio guztiak.
- SIMATIC WinCC V7.3 eta ondorengoak, bertsio guztiak.
- SIMATIC WinCC V7.4, V7.3 eta V7.2, bertsio guztiak.
- SIMATIC WinCC V7.5, 7,5 Upd3 bertsioa baino lehenagoko guztiak.
- SIMATIC PCS 7 V8.0 eta lehenagokoak, bertsio guztiak.
- SIMATIC PCS 7 V8.1 eta ondorengoak, bertsio guztiak.
- SIMATIC PCS V7.2 eta lehenagoko bertsio guztiak.
- SIMATIC WinCC V7.3 eta ondorengo bertsio guztiak.

- SIMATIC HMI Comfort Panels 4" - 22". V15.1 Update 1 baino lehenagoko bertsio guztiak.
- SIMATIC HMI Comfort Outdoor Panels 7" & 15". V15.1 Update 1 baino lehenagoko bertsio guztiak.
- SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 und KTP900F. V15.1 Update 1 baino lehenagoko bertsio guztiak.
- SIMATIC WinCC Runtime Advanced, Professional eta TIA Portal. V15.1 Update 1 baino lehenagoko bertsio guztiak.
- SIMATIC HMI Classic Devices (TP/MP/OP/MPMobile Panel). Bertsio guztiak.
- SISHIP EMCS, IMAC eta IPMS: Bertsio guztiak.

Azalpena:

Kaspersky Lab ICS CERTeko Vladimir Dashchenko eta Sergey Temnikov ikertzaileek, ZheJiang Guoli Security Technology-ko ChengBin Wang ikertzaileak, SySS GmbH eta axt-ko Manuel Stotz eta Matthias Deeg ikertzaileek, iDefense Labs enpresak eta CNCERT/CC-k, bai eta Siemens berak ere, Siemensen zenbait produkturi eragiten dieten hainbat ahultasun aurkitu dituzte, era hauetakoak: informazioaren hedapena, memoria hondatzea, bufferraren gainezkatzea, konfigurazio desegokia, pasahitz barneratuak, zifratze desegokiaren erabilpena, XSS, komunikazioak garbian, akatsa fitxategiak kargatzean, komandoen injekzioa eta abar. Erasotzaile batek gailua berrabiaraz lezake, zerbitzuaren ukapen egoera eragin, komandoak exekutatu edo informazio sentikorra eskuratu.

Konponbidea:

- SCALANCE W1750Dren kasuan, bertsio berrira eguneratzea.
- SINAMICS PERFECT HARMONY GH180 Drives NXG I eta NXG IIren kasuan, NXGpro control-era eguneratzea.
- Siemens-en SISHIP Automation-en kasuan, WibuKey-k egindako bertsiora eguneratzea.
- SIMATIC WinCC (ITA Portal) eta SIMATIC HMIren kasuan, V15.1 Update 1 edo goragoko bertsiora eguneratzea.
- Siemensek eguneraketa berririk ez duen gailuen kasuan, arintze neurri batzuk eta praktika on batzuk gomendatzen ditu:
  - Soilik baliozkotutako iturrietatik datozen proiektuak irekitzea.
  - Gidaliburuetan azaldutako zibersegurtasun kontzeptuak aplikatzea.
  - Defentsa sakonaren printzipioak aplikatzea.
  - SIMATIC WinCC eta SIMATIC PCS 7-ren arteko komunikazioetarako kanal zifratuak ezartzea, '*Encrypted communication*'.
  - Kaltetutako gailuek web zerbitzuetara duten sarbidea murriztea.
  - 161/UDP atakarako sarbidea baliozkotutako gailuek soilik izatea.
  - *Fieldbus-en* parametroan Irakurketa/Idazketa funtzionaltasuna desgaitzea.

Xehetasuna:

Larritasun kritikoko ahultasunak honako hauek dira:

- Kaltetutako gailua dagoen sarera 10005/TCP atakatik sarbidea lukeen autentifikaziorik gabeko erasotzaile batek birkonfigurazio ekintzak egin litzake, eta gailuak dituen proiektuetako fitxategiak eskura litzake. Ahultasun honek eragina dauka kaltetutako gailuaren konfidentzialtasun, integritate eta eskuragarritasunean. Ahultasun horretarako CVE-2019-10919 identifikatzailea erreserbatu da.
- Kaltetutako gailuaren web zerbitzura sarbidea lukeen erasotzaile batek komandoak injekta litzake autentifikatuta egon behar izan gabe. Horren ondorioz, kaltetutako gailuaren sistema eragilean komandoen exekuzio arbitrarioa egin lezake, eta horrela fitxategiak kopiatu, konfigurazioak irakurri, fitxategiak idatzi, fitxategiak ezabatu edo gailua berrabiarazi. Ahultasun horretarako CVE-2018-7084 identifikatzailea erabili da.
- Datu basea duen zerbitzarian sarbide lokala eta baimenak dituen erasotzaile batek sisteman komandoak exekuta litzake. Ahultasun honek eragina dauka kaltetutako sistemaren konfidentzialtasun, integritate eta eskuragarritasunean. Ahultasun horretarako CVE-2019-10916 identifikatzailea erreserbatu da.
- Komunikazio zifratuak erabiltzen ez dituen kaltetutako gailua dagoen sarera sarbidea lukeen autentifikatu gabeko erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun honek eragina dauka kaltetutako sistemaren konfidentzialtasun, integritate eta eskuragarritasunean. Ahultasun horretarako CVE-2019-10922 identifikatzailea erreserbatu da.
- Erasotzaile batek bereziki diseinatutako IRP pakete bat (E/S eskaerak) bidal lezake bufferraren gainezkatzea eragingo lukeena. Horrela kernel-aren memoria hondatzea eta sisteman pribilegioen eskalatzea gertatuko lirateke. Ahultasun horretarako CVE-2018-3990 identifikatzailea erabili da.
- Erasotzaile batek bereziki diseinatutako TCP pakete bat bidal lezake, horrela bufferraren gainezkatzea eragin eta baita kodearen urruneko exekuzioa ere. Ahultasun horretarako CVE-2018-3991 identifikatzailea erabili da.

Gainerako ahultasunetarako erabilitako identifikatzaileak honakoak dira: CVE-2019-10924, CVE-2019-10920, CVE-2019-10921, CVE-2018-7083, CVE-2018-16417, CVE-2018-7082, CVE-2019-6578, CVE-2019-10918, CVE-2019-6574, CVE-2018-7064, CVE-2019-6572, CVE-2019-6576, CVE-2019-6577, CVE-2019-10917 eta CVE-2018-3989.

Etiketak: Eguneraketa, Komunikazioak, SCADA, Siemens, Ahultasuna

---

Baliozkotu gabeko bilaketa ibilbidea Omron-en DeviceNet-en Network Configurator-en

Argitalpen data: 2019/05/15

Garrantzia: Handia

Kaltetutako baliabideak:

- DeviceNet Safety-ren Network Configurator, 3.41 eta lehenagoko bertsioak.

Azalpena:

n0b0dy ikertzaileak, NCCICrekin batera, baliozkotu gabeko bilaketa ibilbidearen erako ahultasun bat aurkitu du Omron-en DeviceNet Safety-ren Network Configurator aplikazioan. Ahultasun horiek arrakastaz baliatuz gero, erasotzaile batek kode arbitrarioa exekuta lezake aplikazioaren pribilegioekin.

Konponbidea:

Omron-ek ez du oraindik argitaratu ahultasun hori konpon dezakeen eguneraketarik. Bitartean, hura arintzeko honako neurrietako bat aplikatzea gomendatzen du:

- PATH ingurunearen aldagaian zerrendatutako direktorioak ezabatzea edo murriztea.
- Sistemaren direktorioen gainean idazketa baimenak soilik administratzaile kontuek dituztela ziurtatzea.
- Windowsen PCak erabiltzaile estandarrekin erabiltzea, administratzaile kontuak kasu berezietarako erabiliz.
- Aplikazioa instalatuta dagoen direktorioaren barnean fitxategi ez fidagarririk ez dagoela ziurtatzea.
- Direktorioan fitxategi ez-fidagarririk ez dagoela ziurtatzea bertan proiektu fitxategi bat exekutatu aurretik, edo bestela karpeta fidagarri batera mugitzea.

Xehetasuna:

- Aplikazioak baliabideak erabiltzen ditu baliozkotu gabeko bilaketa ibilbide batean. Hori baliatuz, asmo gaiztoko DLL fitxategi bat exekuta liteke aplikazioak kontrolatzen ez duen leku batean kokatuta dagoena eta aurreikusitako direktorioetatik kanpo. Ahultasun horretarako CVE-2019-10971 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna

Múltiples vulnerabilidades en productos Schneider Electric

Argitalpen data: 2019/05/16

Garrantzia: Handia

Kaltetutako baliabideak:

- Modicon M580, V2.50, V2.80 eta V2.30 *firmware*-duna baino lehenagokoa.
- Modicon M340, V3.01 *firmwarearen* aurreko bertsio guztiak.
- BMxCRA312XX, V2.40 baino lehenagoko *firmware*-duna.
- Modicon Premium, bertsio guztiak.
- 140CRA312xxx, bertsio guztiak.
- Modicon Quantum, V2.40 bertsioa baino lehenagoko *firmwarearen* bertsio guztiak.
- TSXETG100, bertsio guztiak.
- BMX-NOR-0200H, V1.7 IR 19 baino lehenagoko *firmware*-duna.
- Floating License Manager, V2.3.0.0 bertsioa eta lehenagokoak.
- Modicon M100, bertsio guztiak.
- Modicon M200,bertsio guztiak.
- ATV IMC drive controller, bertsio guztiak.
- Modicon M241, bertsio guztiak.
- Modicon M251, bertsio guztiak.
- Modicon M258, bertsio guztiak.
- Modicon LMC058,bertsio guztiak.
- Modicon LMC078,bertsio guztiak.
- PacDrive Eco, bertsio guztiak.
- PacDrive Pr, bertsio guztiak.
- PacDrive Pro2,bertsio guztiak.
- NET55XX Enconder, bertsioa baino lehenagoko *firmware*-duna.

Azalpena:

Positive Technologies, VAPT Team (C3i IITK, UP, India), CNCERT/CC, Fortiphyd Logic eta Claroty konpainietako hainbat ikertzailek, Schneider Electric-ekin lankidetzan, Schneider Electric-en zenbait produkturi eragiten dieten era ezberdinetako hainbat ahultasunen berri eman dute: zerbitzuaren ukapena, kodearen injekzioa, Cross-Site Scripting (XSS), kredentzial barneratuak, aski ausazkoak ez diren balioak eta funtzio kritikoan autentifikaziorik eza. Erasotzaile batek honako hau egin lezake: zerbitzuaren ukapen egoera eragin, erabiltzailearen testuinguruan scriptak exekutatu, FTP zerbitzura baimenik gabe sartu, TCP konexioa bahitu eta gailuaren IP konfigurazioa aldatu, eta produktuaren konfidentzialtasun, integritate eta eskuragarritasunean eragin.

Konponbidea:

- Modicon M580: V2.80 bertsiora eguneratzea
- Modicon M340: V3.01 bertsiora eguneratzea.
- BMX/E CRA: V2.40 bertsiora eguneratzea.
- Modicon Quantum: V3.5x bertsiora eguneratzea.
- Floating License Manager: V2.3.1.0 bertsiora eguneratzea.
- NET55XX Encoder: 2.1.9.7 bertsiora eguneratzea.

Eguneraketarik ez duten gailuen kasuan Schneider-ek honako hau gomendatzen du:

- Sarea segmentatzea eta TCP 502 eta 4418 eta UDP 2222, 27126 eta 27127 atakak suebakian blokeatzea.
- Aplikazio suebaki bat erabiltzea erabiltzaileen sarrera datuak egiaztatzeko edo suebaki estandar bat erabiltzea HTTP trafikoa eta baimenik gabeko sarbideak mugatzeko TSXETG100 produktura.
- TCP ataketarako kanpoko trafiko guztia suebakian blokeatzea eta sarbide kontroleko zerrenda bat konfiguratzea.
- 'Auto Discovery protocol enable' aukera desgaitzea.
- 'Discovery protocol active' aukera desgaitzea.

Xehetasuna:

Larritasun kritikoko ahultasunak honako hauek dira:

- Urruneko erasotzaile batek, sarbide kontrol oker baten bidez, konfidentzialtasuna, integritatea eta eskuragarritasuna arriskuan jar litzake webUI-ra asmo gaiztoko eskari bat bidaliz. Ahultasun horretarako CVE-2019-6814 identifikatzailea erreserbatu da.
- Urruneko erasotzaile batek kode arbitrarioa exekuta lezake Imadmin osagaian eta FlexNet Publisher-en Daemon-en, esleitutako edo esleipena kendutako memoria aldatuz eta Daemon-en nahitaezko itxiera eraginez. Ahultasun horretarako CVE-2018-20033 identifikatzailea erreserbatu da.

Honako hauek dira larritasun altuko ahultasunak:

- Funtzio kritiko batean autentifikaziorik ez egotea balia lezake erasotzaile batek kaltetutako gailuaren IP konfigurazioa aldatzeko (IP helbidea, sare maskara edo pasabidearen IP helbidea), Ethernet bilbe zehatz bat jasotzean. Ahultasun horretarako CVE-2019-6820 identifikatzailea erreserbatu da.
- Urruneko erasotzaile batek zerbitzuaren ukapena eragin lezake Imadmin osagaira edo FlexNet Publisher-en Daemon-era mezu bat bidaliz. Horrela Daemon-aren nahitaezko itxiera eragin lezake. Ahultasun horietarako CVE-2018-20034, CVE-2018-20031 eta CVE-2018-20032 identifikatzaileak erreserbatu dira.
- Erasotzaile batek zerbitzuaren ukapena eragin lezake telnet konexio bat erabiltzean, kredentzialen administrazioan dagoen ahultasun bat baliatuz. Ahultasun horretarako CVE-2018-7788 identifikatzailea erreserbatu da.
- Erasotzaile batek zerbitzuaren ukapen egoera eragin lezake edo baimenik gabeko aldaketak egin PLCren konfigurazioan Ethernet/IP protokoloa erabiliz, baimenetan, pribilegioetan eta sarbide kontrolean dagoen ahultasun bat baliatuz. Ahultasun horretarako CVE-2018-6815 identifikatzailea erreserbatu da.
- Erasotzaile batek kodea injekta lezake eta *firmwarearen* baimenik gabeko aldaketa eta zerbitzuaren ukapena eragin litzake,

Modbus protokoloa erabiltzean. Ahultasun horretarako CVE-2018-6816 identifikatzailea erreserbatu da.
- Ezohikoak diren baldintzen egiaztapen desegokiaren bidez, erasotzaile batek zerbitzuaren ukapena eragin lezake Modbus bilbe bereziak bidaliz kontrolatzailera. Ahultasun horretarako CVE-2018-6819 identifikatzailea erreserbatu da.

Gainerako ahultasunetarako erabilitako identifikatzaileak honako hauek dira: CVE-2018-7851, CVE-2018-7834, CVE-2018-6812 eta CVE-2018-6821.

Etiketak: Eguneraketa, Schneider Electric, Ahultasuna

Mugez kanpoko irakurketa Fuji Electric-en Alpha7 PC Loader-en

Argitalpen data: 2019/05/17

Garrantzia: Txikia

Kaltetutako baliabideak:

- Alpha7 PC Loader, 1.1 eta lehenagoko bertsioak.

Azalpena:

9SG Security Team-eko kimiya segurtasun ikertzaileak, Trend Micro-ko Zero Day Initiative-rekin lankidetzan, mugez kanpoko irakurketa erako ahultasun baten berri eman du. Ahultasun hori arrakastaz baliatuz gero, erasotzaile batek funtzionamendu okerra eragin lezake kaltetutako gailuan.

Konponbidea:

- Fabrikatzaileak gomendatzen du kaltetutako gailuaren softwarea 1.2 bertsiora eguneratzea, ahultasun hori konpontzen baitu.

Xehetasuna:

- Mugez kanpoko irakurketa erako ahultasun hori arrakastaz baliatuz gero, erasotzaile batek gailuaren portaera okerra eragin lezake, eta horrela sistemaren ustekabeko itxiera gertatuko litzateke. Ahultasun horretarako CVE-2019-10975 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

CAPICOM liburutegiak duen ahultasun batek Yokogawa produktuei eragiten die

Argitalpen data: 2019/05/17

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- CENTUM:
  - CENTUM VP (R5.02.00 - R6.04.00)
  - CENTUM VP Entry Class (R5.02.00 - R6.04.00)
- STARDOM (R3.20 - R4.20)
- B/M9000 VP (R7.02.01 - R8.02.02)

Azalpena:

Yokogawa-k CAPICOM liburutegiaren erabilpena identifikatu du bere produktu batzuetan. Liburutegi kriptografiko horrek duen ahultasuna baliatuz erasotzaile batek urruneko kodea exekuta lezake.

Ebazpena:

- Fabrikatzaileak gomendatzen du CAPICOM liburutegia ezabatzea segurtasun arazo hau konpontzeko.

Xehetasuna:

- CAPICOM liburutegi kriptografikoak duen ahultasuna baliatuz erasotzaile batek urruneko kodea exekuta lezake. Ahultasun horretarako CVE-2007-0940 identifikatzailea erabili da.

Etiketak: Ahultasuna

Microsoft Windows RDS (Remote Desktop Service) erako ahultasuna Kontrol Industrialeko Sistemetan

Argitalpen data: 2019/05/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

RDS zerbitzuak duen ahultasun honek eragin egin die Kontrol Industrialeko sistemen produktuen fabrikatzaileei, honako hauei besteak

beste:

- Siemens Healthineers gamako hainbat produktu.
- Sistema Eragile modura Microsoft Windows erabiltzen duten Schneider Electric-en hainbat produktu.

Azalpena:

Maiatzean argitaratutako Microsoft-en segurtasun eguneraketen argitalpenak RDS (*Remote Desktop Service*) zerbitzuari eragiten dion ahultasun baten berri ematen du. Horrek eragin egingo lieke zerbitzu hori erabiltzen duten hainbat produktu industriali, esate baterako Siemens Healthineers gamari eta Schneider Electric-en hainbat produkturi. Ahultasun hori baliatuz, autentifikaziorik gabeko urruneko erasotzaile batek urruneko kodea exekuta lezake xede den sisteman, sistema horrek Microsoft Windows-en RDS (*Remote Desktop Service*) zerbitzurako sarbidea saretik egiteko aukera badu. Ohartarazpen hau aurretik ere argitaratua izan zen INCIBE-CERTen IT sistemen kasurako, era honetara: Microsoft-en 2019ko maiatzeko segurtasun buletina.

Ebazpena:

- Microsoft-ek eguneraketa bat dauka kaltetutako sistema eragileentzat, RDSk (*Remote Desktop Service*) duen ahultasuna konpontzen duena.

Xehetasuna:

- Microsoft Windows-en RDS (*Remote Desktop Service*) zerbitzuan aurkitu den ahultasuna baliatuz, autentifikatu gabeko urruneko erasotzaile batek kodea exekuta lezake. Erasotzaileak sarerako sarbidea izan beharko luke, eta sistemak RDS zerbitzua agerian izan, normalean 3389/TCP atakatik. Bereziki diseinatutako RDP eskaerak bidaliz erasotzaileak ahultasun hori balia lezake, eta besteak beste, programak instala litzake, kontuak sortu edo kodea urrunetik exekutatu. Ahultasun horretarako CVE-2019-0708 identifikatzailea erabili da.

Etiketak: Eguneraketa, Microsoft, Schneider Electric, Siemens, Ahultasuna, Windows

---

Intel produktuek duten ahultasun batek Kontrol Industrialeko Sistemei eragiten die

Argitalpen data: 2019/05/20

Garrantzia: Handia

Kaltetutako baliabideak:

- Intel-en arabera, honako da kaltetutako CPUen zerrenda.

CPUek dituzten ahultasun horiek eragin egin diete kontrol industrialeko sistemen produktuen fabrikatzaileei, honakoei besteak beste:

- Schneider Electric.

Azalpena:

Intel-en CPU gama zabal bati eragiten dion segurtasun ahultasun batek hainbat produktu arriskuan jarri ditu. Ahultasun hori arrakastaz baliatuz gero erasotzaile batek beste prozesu batzuetako informazio sentikorrera sarbidea lor lezake edo beste pribilegio batzuekin sartzea izatea. Ohartarazpen hau aurretik ere argitaratua izan zen INCIBE-CERTen IT sistemen kasurako, era honetara: Hainbat ahultasun Intel produktuetan.

Konponbidea:

- Produktuaren azken bertsiora eguneratzea hemen: Intel-en softwarearen deskarga zentroa.

Xehetasuna:

- Microarchitectural Data Sampling (MDS) ahultasuna baliatuz, ZombieLoad, FallOut edo RIDL ere izendatua, sistema lokal batean kodearen exekuzio baimenak lituzkeen erasotzaile batek ahultasun hori balia lezake babestuta dauden sistemaren datuetara edo sarbiderik izan behar ez lukeen datuetara sartzeko. Ahultasun horietarako honako identifikatzaileak erabili dira: CVE-2018-12126, CVE-2018-12130, CVE-2018-12127 eta CVE-2019-11091.

Etiketak: Eguneraketa, Schneider Electric, Ahultasuna

Hainbat ahultasun Miele-ren XGW 3000 ZigBee Gateway-n

Argitalpen data: 2019/05/21

Garrantzia: Ertaina

Kaltetutako baliabideak:

- XGW 3000 ZigBee Gateway.

Azalpena:

Maxim Rupp ikertzaileak Miele-ren XGW 3000 ZigBee Gateway produktuari eragiten dioten bi ahultasunen berri eman du, bat CSRF (*Cross-site request forgery*) erakoa eta bestea autentifikazioaren saiheste erakoa.

Konponbidea:

- Softwarearen 2.4.0 bertsioa instalatzea XGW 3000 ZigBee Gateway-ren eguneratze automatikoaren funtzioaren bitartez.

Xehetasuna:

- Autentifikatutako erabiltzaile administratibo batek bisitatzen duen asmo gaiztoko webgune batek edo asmo gaiztoko email batek aldaketa arbitrarioak egin ditzakete admin *panel-ean* CSRF eraso baten bidez.
- Aurreko ahultasunarekin batera, administratzaile pasahitza alda daiteke zaharra egiaztatu gabe, era horretara saihestuz pasahitz aldaketaren funtzioa.

Etiketak: Eguneraketa, Ahultasuna

+Baliabideen kontrolik gabeko kontsumoa Mitsubishi Electric-en MELSEC-Q Series-en

Argitalpen data: 2019/05/22

Garrantzia: Handia

Kaltetutako baliabideak:

- MELSEC-Q Series-en Ethernet QJ71E71-100 modulua, 20121 eta lehenagoko serie zenbakiduna.

Azalpena:

Nozomi Networds-eko Younes Dragoni eta Alessandro Di Pinto ikertzaileek baliabideen kontrolatu gabeko kontsumo erako ahultasun baten berri eman dute. Erasotzaile batek ahultasun hau arrakastaz baliatuz gero, gailuak ez erantzutea eragin dezake, eta PLCa fisikoki berrabiarazi beharko litzateke.

Konponbidea:

- Ahultasun hori konpontzeko fabrikatzaileak gomendatzen du QJ71E71-100 modulua *firmware-aren* 20122 bertsiora eguneratzea.

Xehetasuna:

- Erasotzaile batek bereziki diseinatutako TCP paketeak bidal litzake FTP zerbitzuaren aurka, eta horrela xede diren gailuak akats moduan sartzea eragingo luke, zerbitzuaren ukapen egoera sortuz. Ahultasun horretarako CVE-2019-10977 kodea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna