2019ko Azaroaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Hainbat ahultasun Honeywell-en produktuetan

Argitalpen data: 2019/11/04

Garrantzia: Altua

Kaltetutako baliabideak:

- equIP Series IP Cameras.
- equIP eta Performance Series IP Cameras eta Recorders.

Azalpena:

Honeywell-eko ekipoak hainbat eratako ahultasunen berri eman du: sarrera okerraren baliozkotzea, funtzio kritikoetarako autentifikaziorik eza eta autentifikazioa saihestea.

Konponbidea:

Honeywell-ek hainbat eguneraketa garatu ditu kaltetutako gailuentzat.

Xehetasuna:

- Kaltetutako produktuek duten ahultasun bat baliatuz, bereziki diseinatutako HTTP pakete baten eskaera baten ondorioz zerbitzuaren ukapen egoera eragin liteke. Ahultasun horretarako CVE-2019-18228 identifikatzailea erabili da.
- Urruneko erasotzaile batek gailuaren audiora sarbidea lor lezake, HTTP eskaera baten bidez, inolako autentifikaziorik gabe. Ahultasun horretarako CVE-2019-18230 identifikatzailea erabili da.
- Errepikatze eraso erako ahultasun bat dago, heredatutako produktuekin bateragarritasuna lortzeko autentifikazio ahuleko metodo bat mantentzen delako. Ahultasun horretarako CVE-2019-18226 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Advantech-en WISE-PaaS/RMM-n

Argitalpen data: 2019/11/04

Garrantzia: Kritikoa

Kaltetutako baliabideak:

WISE-PaaS/RMM, 3.3.29 eta lehenagoko bertsioak.

Azalpena:

9sg Security Team-eko rgod ekipoak eta trendytofu-k lau ahultasunen berri eman dute, bi larritasun kritikokoak, bat altukoa eta bestea ertainekoa. Urruneko erasotzaile batek administratzaile pribilegioekin kodea urrunetik exekutatzea eragin lezake, autentifikaziorik gabe funtzioak erabili, informazio sentikorrera sarbidea lortu eta SQL komandoak injektatu.

Konponbidea:

Advantech-ek 2019ko uztailean WISE-PaaS/RMM ordeztu egin du EdgeSense eta DeviceOn-ekin, eta kaltetutako softwarea berriarekin ordezkatzea gomendatzen dute, berriak zerbitzua baitu.

Xehetasuna:

- Larritasun kritikoko ahultasunak honakoak dira:
  - Direktorioen bideetako baliozkotze gabezia baliatuz, erasotzaile batek urruneko kodea exekuta lezake, administratzailea

balitz bezala jokatuta. Ahultasun horretarako CVE-2019-13551 identifikatzailea erabili da.
    - IP helbidera sartzea lortzen duen edozeinek erabil dezakeen funtzio bat dago, autentifikazioaren beharrik gabe erabil daitekeena. Ahultasun horretarako CVE-2019-13547 identifikatzailea erabili da.
- Kritikotasun altuko ahultasuna honakoa da:
    - XXE erako hainbat ahultasun daude, eta horiek baliatuz erasotzaile batek informazio sentikorra ezagutzera eman lezake. Ahultasun horretarako CVE-2019-18227 identifikatzailea erabili da.
- Kritikotasun ertaineko ahultasuna honakoa da:
    - Erabiltzailearen sarreren tratamendurik eza baliatuz, erasotzaile batek SQL komandoak injekta litzake, eta horren bidez informazio sentikorra ezagutzera eman lezake. Ahultasun horretarako CVE-2019-18229 identifikatzailea erabili da.

Etiketak: Ahultasuna

Autentifikazio gabezia ABBren hainbat produktutan

Argitalpen data: 2019/11/04

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Power Generation Information Manager (PGIM), bertsio guztiak,
- Plant Connect, bertsio guztiak.

Azalpena:

Bodforss Consulting-eko Rikard Bodforss ikertzaileak ABBren produktuek duten ahultasun kritiko baten berri eman du. Urruneko erasotzaile batek autentifikazioa saihets lezake, kredentzialak atera, eta PGIM History-ren konfigurazioa eta datu baseko gertakariak aldatu.

Konponbidea:

ABBk gomendatzen du produktu eguneratua erabiltzea, Symphony Plus Historian. Dagoeneko erabilgarri dago eta ahultasun hori konpontzen du.

Xehetasuna:

Erabiltzailearen kredentzialen eta autentifikazio mekanismoen babes ez-nahikoak baliatuz, urruneko erasotzaile batek PGIMen erabiltzailearen kredentzialak eskura litzake, eta ondoren, bai PGIMen konfigurazioa eta bai datu basea alda litzake.

Etiketak: Ahultasuna

Funtzio zaharkituaren erabilpen erako ahultasuna Omron-en CX-Supervisor-en

Argitalpen data: 2019/11/06

Garrantzia: Altua

Kaltetutako baliabideak:

CX-Supervisor, 3.5 (12) eta lehenagoko bertsioak.

Azalpena:

Micro's Zero Day Initiative-ko Michael DePlante ikertzaileak funtzio zaharkituaren erabilpen erako ahultasun baten berri eman du.

Konponbidea:

CX-Supervisor 3.51 (9) bertsiora eguneratzea.

Xehetasuna:

CX-Supervisor sisteman funtzio zaharkitua erabiltzen denez, urruneko erasotzaile batek ahultasun hori balia lezake, eta horrela informazio sentikorrera sarbidea lortu, sistema osoa arriskuan jarri, eta ekipoa erabilgarri ez egotea eragin. Gainera Omron CX-Supervisor Teamviewer 5.0.8703 QSrekin batera saltzen da, eta bertsio horrek ezagunak diren hiru ahultasun ditu. Ahultasun horretarako CVE-2019-11769, CVE-2018-16550, CVE-2018-14333 eta CVE-2010-3128 identifikatzaileak erabili dira.

Etiketak: Eguneraketa, Azpiegitura kritikoak, Ahultasuna

Hainbat ahultasun Moxa-ren EDS-405A Series-en

Argitalpen data: 2019/11/07

Garrantzia: Altua

Kaltetutako baliabideak:

EDS-405A Series, 3.8 bertsioa eta lehenagokoak.

Azalpena:

Moxa-ko taldeak bere web zerbitzuetako batek duen zerbitzuaren ukapen erako ahulezien berri eman du. Hori baliatuz urruneko

erasotzaile batek gailua erabilezin utz lezake, erabiltzaile baimenduak gailura sartzeko gaitasunik gabe utziz.

Konponbidea:

Segurtasun partxea aplikatzea.

Xehetasuna:

- Bereziki diseinatutako HTTP GET komando bat bidaliz, urruneko erasotzaile batek zerbitzuaren ukapen egoera eragin lezake. Hau gertatzen da paketearen payload-aren tamaina ez delako egiaztatzen.

Etiketak: Eguneraketa, Ahultasuna

Bufferraren gainezkatzea Fuji Electric-en V-Server ekipamenduan

Argitalpen data: 2019/11/08

Garrantzia: Altua

Kaltetutako baliabideak:

V-Server, 4.0.6 bertsioa eta lehenagokoak.

Azalpena:

9SG-ko Kimiya-k, Trend Micro's Zero Day Initiative-rekin batera, kritikotasun altuko ahultasun bat aurkitu du. Urruneko erasotzaile batek gailuan ustekabeko itxiera edo kode arbitrarioaren exekuzioa eragin litzake.

Konponbidea:

Fuji Electric-ek ahultasun hori konpontzeko 4.0.7.0 bertsioa argitaratu du.

Xehetasuna:

Ahultasunaren jatorria pilan oinarritutako bufferraren hainbat gainezkatze dira. Urruneko erasotzaile batek gailuan ustekabeko itxiera edo kode arbitrarioaren exekuzioa eragin litzake. Ahultasun horretarako CVE-2019-18240 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Baliabideen kontrolik gabeko kontsumoa Mitsubishi Electric-en hainbat produktutan

Argitalpen data: 2019/11/08

Garrantzia: Altua

Kaltetutako baliabideak:

- MELSEC-Q Series:
  - 21081 serie zenbakia edo lehenagokoa duten Q03/04/06/13/26UDVCPU;
  - 21081 serie zenbakia edo lehenagokoa duten Q04/06/13/26UDPVCPU;
  - 21081 serie zenbakia edo lehenagokoa duten Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU.
- MELSEC-L Series:
  - 21101 serie zenbakia edo lehenagokoa duten L02/06/26CPU L26CPU-BT;
  - 21101 serie zenbakia edo lehenagokoa duten L02/06/26CPU-P L26CPU-PBT;
  - 21101 serie zenbakia edo lehenagokoa duten L02/06/26CPU-CM L26CPU-BT-CM.

Azalpena:

Amazon's Customer Fulfillment Technology Security-ko Tri Quach-ek baliabideen kontrolik gabeko kontsumo erako ahultasun baten berri eman du. Ahultasun hori arrakastaz baliatuz gero kaltetutako produktuetan FTP bezeroa FTP zerbitzarira konekta dadin eragotz dezake.

Konponbidea:

Mitsubishi Electric-ek *firmware*-aren bertsio berria argitaratu du ahultasuna konpontzeko. Horrez gain, Mitsubishi Electric-ek erabiltzaileei gomendatzen die gailu hori *firewall* baten bitartez erabiltzeko.

Xehetasuna:

Urruneko erasotzaile batek FTP zerbitzuak zerbitzuaren ukapen egoera eragitea lor lezake, kaltetutako CPU moduluetan FTP zerbitzarira erasotzailea konektatzen den unearen arabera. Ahultasun honek FTP zerbitzariaren funtzioari soilik eragiten dio. Ahultasun horretarako CVE-2019-13555 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Medtronic-en Valleylab produktuetan

Argitalpen data: 2019/11/08

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Valleylab LS10 Energy Platform (VLLS10GEN), 1.20.2 eta lehenagoko bertsioak;
- Valleylab Exchange Client, 3.4 eta lehenagoko bertsioak;
- Valleylab FT10 Energy Platform (VLFT10GEN), 4.0.0 eta lehenagoko bertsioak;
- Valleylab FX8 Energy Platform (VLFX8GEN), 1.1.0 eta lehenagoko bertsioak.

Azalpena:

Medtronic-eko ekipoak era ezberdinetako ahultasunen berri eman du: autentifikazio okerra, babes mekanismoaren akatsa, kodetutako kredentzialen erabilpena, *hash* algoritmo alderantzikagarrien erabilpena eta sarreren baliozkotze okerra. Ahultasun horiek baliatuz gero, urruneko erasotzaile batek tresna ez-seguruak konekta litzake sistemaren integritatea galduz, fitxategiak gainidatzi edo kodea urrunetik exekutatu.

Konponbidea:

Medtronic-ek gomendatzen du ahultasun horiek konpontzeko eskuragarri dauden bertsio berrietara eguneratzea, eta eurekin harremanetan jartzea partxe berriak eskuratzeko.

Xehetasuna:

- FT10/LS10 Energy Platform gailuetako autentifikaziorako erabilitako RFID segurtasun mekanismoa saihets daiteke, eta horrela tresna ez-originalak edo benetakoak ez direnak konekta daitezke sortzailera. Ahultasun horretarako CVE-2019-13531 identifikatzailea erreserbatu da.
- RFID segurtasun mekanismoak ez du irakurketa babesik ezartzen, eta horrek RFID segurtasun mekanismoaren datuetara irakurketa sarbide osoa ahalbidetzen du. Ahultasun horretarako CVE-2019-13535 identifikatzailea erreserbatu da.
- Kaltetutako produktuek kodetutako kredentzialen hainbat multzo erabiltzen dituzte. Antzematen badira, gailuan fitxategiak irakurtzeko erabil daitezke. Ahultasun horretarako CVE-2019-13543 identifikatzailea erreserbatu da.
- Kaltetutako produktuek deskribapen algoritmoa erabiltzen dute sistema eragileko pasahitzen *hash*-erako. Sarean oinarritutako saio interaktiboen hasierak desaktibatuta dauden bitartean, erasotzaileek azaldutako beste ahultasunak balia ditzakete *shell*-era sarbide lokala eskuratzeko eta *hash*-etara sarbidea lortzeko. Ahultasun horretarako CVE-2019-13539 identifikatzailea erreserbatu da.
- Kaltetutako produktuek *rssh*-ren bertsio ahulak erabiltzen dituzte fitxategien igoera ahalbidetzeko. Hori baliatuz, administratzaile baimenak lituzkeen erasotzaile batek fitxategietara sarbidea lor lezake edo kodea exekuta lezake ausaz. Ahultasun horretarako CVE-2019-3464 eta CVE-2019-3463 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, Osasuna, Ahultasuna

Hainbat ahultasun Siemensen produktuetan

Argitalpen data: 2019/11/12

Garrantzia: Altua

Kaltetutako baliabideak:

- Nucleus NET: bertsio guztiak;
- Nucleus RTOS: bertsio guztiak;
- ARM, MIPS eta PPCrako Nucleus ReadyStart: 2017.02.2 baino lehenagoko bertsio guztiak;
- Nucleus SafetyCert: bertsio guztiak;
- Nucleus Source Code: bertsio guztiak;
- VSTAR: bertsio guztiak;
- CPU S7-1200:bertsio guztiak;
- Designo PX automatizazio kontrolatzaileak, 6.00.320 baino lehenagoko *firmware* bertsio guztiak, ondoko produktuen kasuan:
  - Desigo PX Web PXA40-W0, PXA40-W eta PXA40-W2 moduluak dituzten PXC00-E.D, PXC50-E.D, PXC100-E.D, PXC200-E.D;
  - PXC00-U, PXC64-U eta PXC128-U, Desigo PX Web PXA30-W0, PXA30-W1 eta PXA30-W2moduluekin;
  - PXC22.1-E.D, PXC36-E.D eta PXC36.1-E.D web zerbitzaria aktibatuta dutenean.

Azalpena:

Siemens gailuei eragiten dieten hainbat ahultasun argitaratu dira. Ahultasun horiek arrakastaz baliatuz gero, autentifikatu gabeko urruneko erasotzaile batek gailuaren integritatea eta eskuragarritasuna kaltetu litzake, zerbitzuaren ukapen egoera eragin eta diagnostiko funtzio osagarrietara sarbidea lortu.

Konponbidea:

- ARM, MIPS eta PPCrako Nucleus ReadyStart: 2017.02.2 bertsiora eguneratzea eta *Nucleus 2017.02.02 Nucleus NET Patch* partxea instalatzea;
- Nucleus SafetyCert: produktu hau ez dago zuzenean eraginda; nolanahi ere, bere *bundle*-ak Nucleus ReadyStart-en kopia bat dauka, hori kaltetuta dago, eta bere konponbidea aurreko *bullet*-ean erakusten da;
- Designo PX automatizazio kontrolatzaileak: 6.00.320 edo ondoreneko bertsioak instalatzea;
- Kaltetutako gainerako produktuen kasuan, Siemens-en ohartarazpen ofizialetako *Workarounds and Mitigations* ataleko gomendioak kontsultatzea.

Xehetasuna:

- Erasotzaile batek gailu baten integritatea eta eskuragarritasuna arriskuan jar litzake bereziki diseinatutako DHCP paketeak bidaliz. Ahultasun horretarako CVE-2019-13939 identifikatzailea erreserbatu da.
- Abiatze prozesua gertatzen den bitartean UART interfazera sarbide fisikoa lukeen erasotzaile batek diagnostiko funtzio osagarrietara sarbidea lor lezake. Ahultasun horretarako CVE-2019-13945 identifikatzailea erreserbatu da.
- Erasotzaile batek zerbitzuaren ukapen egoera eragin lezake gailuaren web zerbitzarian, bereziki diseinatutako HTTP paketeak bidaliz web zerbitzariaren atakara (tcp/80).Ahultasun horretarako CVE-2019-13927 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Siemens, Ahultasuna

Kodearen exekuzio arbitrarioa ABBren Automation Builder eta Drive Application Builder-en

Argitalpen data: 2019/11/14

Garrantzia: Altua

Kaltetutako baliabideak:

- Automation Builder, 2.3.0 baino lehenagoko bertsio guztiak (PLC AC500 V3 edo IEC61131 unitate programagarriak programatzeko erabiltzen denean soilik).
- Drive Application Builder: 1.0.0 bertsioa.

Azalpena:

WRH Walter Reist Holding AGSe-ko Heinz Füglister ikertzaileak kodearen injekzio erako ahultasuna aurkitu du, ABBren hainbat gailuri eragiten diena. Erasotzaile batek kode arbitrarioa exekuta lezake.

Konponbidea:

ABBk ahultasun hori konpontzen duten eguneraketa bereziak argitaratuko ditu kaltetutako produktu bakoitzerako. Eskuragarri daudenean bertsio horretara eguneratzea gomendatzen da.

- Automation Builder, 2.3.0 bertsiora eguneratzea, 2020ko lehen lauhilekorako eskuragarri.
- Drive Application Builder, 1.1.0 bertsiora eguneratzea, 2019. urte amaierarako eskuragarri.

Eguneraketak argitaratu bitartean, ABBk gomendatzen du iturri fidagarrietatik eskuratutako IEC 61131 liburutegiak soilik erabiltzea.

Xehetasuna:

Ahultasuna IEC 61131-3 liburutegiaren dokumentazioko osagai aktiboetan sortzen da.Garapen ingurunean osagai aktibo horiek inolako baliozkotze prozesurik gabe erakusten dira, eta hori baliatuz erasotzaile batek JavaScript edo ActiveX kodea exekuta lezake.

Etiketak: Eguneraketa, Ahultasuna

Zifratze maila desegokia Philips-en IntelliBridge-n

Argitalpen data: 2019/11/15

Garrantzia: Ertaina

Kaltetutako baliabideak:

- IntelliBridge EC40 Hub, bertsio guztiak;
- IntelliBridge EC80 Hub, bertsio guztiak.

Azalpena:

Ahultasun hau arrakastaz baliatuz gero, erasotzaile batek IntelliBridge-ren EC40/80 *hub*-era baimenik gabeko sarbidea lor lezake. Horrek aukera emango lioke softwarea exekutatzeko, sistemaren konfigurazioa aldatzeko edo fitxategiak ikusi eta eguneratzeko, identifikagarriak ez diren pazienteen datuak barne.

Konponbidea:

Philips-ek ahultasun hori konpontzeko bertsio berri bat argitaratzeko asmoa du 2020ko hirugarren hiruhilekoan.

Xehetasuna:

Kaltetutako produktuetan exekutatzen den SSH zerbitzaria zifratu ahula onartzeko konfiguratuta dago. Hori baliatuz, sarera sarbidea lukeen baimenik gabeko erasotzaile batek saioa harrapatu eta erreproduzitu lezake, eta EC40/80 *hub*-era baimenik gabeko sarbidea lortu.Ahultasun horretarako CVE-2019-18241 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Osasuna, Ahultasuna

Funtzio zaharkituaren erabilpen erako ahultasuna Omron-en CX-Supervisor-en

Argitalpen data: 2019/11/15

Garrantzia: Altua

Kaltetutako baliabideak:

CX-Supervisor, 3.5 (12) eta lehenagoko bertsioak.

Azalpena:

Trend Micro's Zero Day Initiative-ko Michael DePlante ikertzaileak funtzio zaharkituaren erabilpen erako ahultasun baten berri eman du, Omron-en CX-Supervisor-i eragiten diona. Urruneko erasotzaile batek informazioa ezagutzera eman lezake edo sistema eta bere eskuragarritasuna arriskuan jarri.

Konponbidea:

CX-Supervisor 3.51(9) bertsiora eguneratzea.

Xehetasuna:

Omron-en CX-Supervisor Teamviewer-en 5.0.8703 QS bertsioarekin zabaltzen da. TeamViewer-en bertsio hori ahula da, zaharkitutako funtzio bat erabiltzen duelako, erabiltzailearen interakzioa behar duena hura baliatu ahal izateko. Urruneko erasotzaile batek informazioa ezagutzera eman lezake edo sistema eta bere eskuragarritasuna arriskuan jarri. Ahultasun horretarako CVE-2019-18251 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, SCADA, Ahultasuna

Hainbat ahultasun Moxa-ren produktuetan

Argitalpen data: 2019/11/20

Garrantzia: Kritikoa

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,
- EDR-810 Series, 5.1 bertsioa eta lehenagokoak.

Azalpena:

Otorio-ko Yuval Ardon eta Matan Dobrushin ikertzaileek, Motherwell Avanced Technologies Cyber Review Team-eko Neil Pope eta Rhys Cable-rekin batera, larritasun kritikoak dituzten ahultasunak aurkitu dituzte Moxa-ren produktuetan. Urruneko erasotzaile batek gailua zerbitzuz kanpo utz lezake, zerbitzuaren ukapen egoera sortu edo komandoak arbitrarioki exekutatu.

Konponbidea:

Moxa-k ahultasunak arintzen dituzten eguneraketak argitaratu ditu:

- EDS-G508E Series, EDS-G512E Series eta EDS-G516E Series produktuen kasuan, Moxa-ren zerbitzu teknikoarekin harremanetan jarri beharra dago eguneraketa eskuratzeko.
- EDR-810 Series gailuaren kasuan firmware berriaren deskarga eskuragarri dago.

Xehetasuna:

- Ahultasunaren jatorria PROFINET DCE-RPC gailuen aurkikuntza paketeak dira. Urruneko erasotzaile batek gailuak erabilezin utz litzake edo beroietan zerbitzuaren ukapen egoera eragin lezake.
- Web erabiltzailearen interfazean (*Web GUI*) erabilitako elementu berezietako saneamendu falta baliatuz, urruneko erasotzaile batek, bereziki sortutako HTTP POST eskaera baten bidez, komandoen exekuzio arbitrarioa egin lezake. Ahultasun horretarako CVE-2019-14374 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Ahultasuna 3S-Smart Software Solutions GmbH-ren CODESYSen web zerbitzarian

Argitalpen data: 2019/11/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Web zerbitzaria (*CmpWebServer* eta *CmpWebServerHandler*) duten CODESYS V3ren exekuzio denborako sistema guztiak kaltetuta daude, 3.5.15.20 baino lehenagoko bertsioak badira, eta zeinahi delarik CPU edo sistema eragile mota:

- BeagleBone-rako CODESYS Control;
- emPC-A/iMX6rako CODESYS Control;
- IOT2000rako CODESYS Control;
- Linuxerako CODESYS Control;
- PLCnext-erako 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.

Azalpena:

OEM eta Tenable-ren bezero batek memoria dinamikoan (*heap*) oinarritutako bufferraren gainezkatze erako ahultasun baten berri eman du, Codesys V3 sistemei eragiten diena.Ahultasun hori arrakastaz baliatuz gero, urruneko erasotzaile batek zerbitzuaren ukapena eragin lezake edo kode arbitrarioa exekutatu.

Konponbidea:

Ahultasun hori konpontzeko 3S-Smart Software Solutions GmbH-k 3.5.15.20 bertsioa argitaratu du.

Xehetasuna:

CODESYSen web zerbitzaria CODESYS WebVisu-k erabiltzen du web nabigatzaile batean CODESYSen bistaratze pantailak erakusteko. Bereziki diseinatutako eskaerak bidaliz, memoria dinamikoan (*heap*) oinarritutako bufferraren gainezkatzea eragin liteke. Aurrerago, horrek web zerbitzaria blokea lezake, zerbitzuaren ukapen egoera eragin edo urrunetik kodea exekutatzeko balia liteke. Web zerbitzaria CODESYSen exekuzio denborako sistemaren parte denez, horren ondorioz exekuzio sistemak bere osotasunean ustekabeko portaera izan lezake. Ahultasun horretarako CVE-2019-18858 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Flexera-ren FlexNet Publisher-en

Argitalpen data: 2019/11/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

FlexNet Publisher, 2018 R3 eta lehenagoko bertsioak.

Azalpena:

Kaspersky-ko Sergey Temnikov ikertzaileak sarreren baliozkotze oker eta memoriaren hondatze erako ahultasunen berri eman du, Flexera-ren FlexNet Publisher-i eragiten diotenak. Ahultasun horiek arrakastaz baliatuz gero, urruneko erasotzaile batek produktua legalki erabiltzeko lizentzia baliagarri bat eskuratzea uka lezake eta kodea urrunetik exekutatu.

Konponbidea:

Flexera-k 2018 R4 edo goragoko bertsiora eguneratzea aholkatzen du.

Xehetasuna:

- Elementuen prebentziozko ezabaketarekin, mezuen deskodetzearekin edo hornitzailearen *lmgrd* eta *daemon* osagaietako zerrenda batera elementu bat gehitzearekin zerikusia duten hainbat ahultasun baliatuz, urruneko erasotzaile batek mezuen konbinaketa bat bidal lezake *lmgrd* edo *daemon*-era, eta horrela hornitzailearen *lmgrd* eta *daemon* osagaien arteko heartbeat-a geldiaraziko luke eta *daemon*-a itzali. Ahultasun horietarako CVE-2018-20031, CVE-2018-20032 eta CVE-2018-20034 identifikatzaileak erabili dira, hurrenez hurren.
- Hornitzailearen *lmgrd* eta *daemon* osagaiek duten ahultasun bat baliatuz, urruneko erasotzaile batek memoria honda lezake memoria esleituz edo memoriaren esleipena kenduz, *lmgrd* edo *daemon* kargatuz, eta *lmgrd* eta *daemon*-en arteko heartbeat-a geldiaraziz. Horrek saltzailearen deamon-a ixtera behartuko luke. Era berean, ahultasun hau balia liteke kodea urrunetik exekutatzeko. Ahultasun horretarako CVE-2018-20033 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna