2020ko Irailaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Gailu legitimo baten ordezpena Mitsubishi Electric markaren hainbat produktutan

Argitalpen data: 2020/09/02

Garrantzia: Handia

Kaltetutako baliabideak:

- Q24DHCCPU-V, bertsio guztiak;
- Q24DHCCPU-VG, bertsio guztiak;
- R12CCPU-V, bertsio guztiak;
- RD55UP06-V, bertsio guztiak;
- RD55UP12-V, bertsio guztiak;
- RJ71GN11-T2, bertsio guztiak;
- RJ71EN71, bertsio guztiak;
- QJ71E71-100, bertsio guztiak;
- LJ71E71-100, bertsio guztiak;
- QJ71MT91, bertsio guztiak;
- RD78Gn(n=4,8,16,32,64), bertsio guztiak;
- RD78GHV, bertsio guztiak.
- RD78GHV, bertsio guztiak.
- NZ2GACP620-60, bertsio guztiak.
- NZ2GACP620-300, bertsio guztiak.
- NZ2FT-MT, bertsio guztiak.
- NZ2FT-EIP, bertsio guztiak.
- Q03UDECPU, 22081 serie zenbakiko eta aurrekoetako lehenengo 5 digituak;
- QnUDEHCPU(n=04/06/10/13/20/26/50/100), 22081 serie zenbakiko eta aurrekoetako lehenengo 5 digituak;
- QnUDVCPU(n=03/04/06/13/26), 22031 serie zenbakiko eta aurrekoetako lehenengo 5 digituak;
- QnUDPVCPU(n=04/06/13/2), 22031 serie zenbakiko eta aurrekoetako lehenengo 5 digituak;
- LnCPU(-P)(n=02/06/26), 22051 serie zenbakiko eta aurrekoetako lehenengo 5 digituak;
- L26CPU-(P)BT, 22051 serie zenbakiko eta aurrekoetako lehenengo 5 digituak;
- RnCPU(n=00/01/02), 18 bertsioa eta aurrekoak;
- RnCPU(n=04/08/16/32/120), 50 bertsioa eta aurrekoak;
- RnENCPU(n=04/08/16/32/120), 50 bertsioa eta aurrekoak;
- RnSFCPU (n=08/16/32/120), bertsio guztiak;
- RnPCPU(n=08/16/32/120), bertsio guztiak;
- RnPSFCPU(n=08/16/32/120), bertsio guztiak;
- FX5U(C)-**M*/**
  - Caso 1: número de serie 17X**** o posteriores: versión 1.210 y anteriores;
  - Caso 2: número de serie 179**** y anteriores: versión 1.070 y anteriores;
- FX5UC-32M*/**-TS, 1.210 bertsioa eta aurrekoak;
- FX5UJ-**M*/**, 1.000 bertsioa;
- FX5-ENET, bertsio guztiak.
- FX5-ENET/IP, bertsio guztiak.
- FX3U-ENET-ADP, bertsio guztiak;
- FX3GE-**M*/**, bertsio guztiak;
- FX3U-ENET, bertsio guztiak.
- FX3U-ENET-L, bertsio guztiak.
- FX3U-ENET-P502, bertsio guztiak.
- FX5-CCLGN-MS, bertsio guztiak.
- IU1-1M20-D, bertsio guztiak.
- LE7-40GU-L, bertsio guztiak.
- GOT2000 Series GT21 Model, bertsio guztiak;
- GS Series, bertsio guztiak;

- GOT1000 Series GT14 Model, bertsio guztiak;
- GT25-J71GN13-T2, bertsio guztiak.
- FR-A800-E Series, bertsio guztiak;
- FR-A800-E Series, bertsio guztiak;
- FR-A8NCG, 2020ko abuztuko ekoizpen data eta aurrekoak;
- FR-E800-EPA Series, 2020ko uztaileko ekoizpen data eta aurrekoak;
- FR-E800-EPA Series, 2020ko uztaileko ekoizpen data eta aurrekoak;
- Conveyor Tracking Application APR-nTR3FH, APR-nTR6FH, APR-nTR12FH, APR-nTR20FH(n=1,2), bertsio guztiak (produktu ez jarraia);
- MR-JE-C, bertsio guztiak;
- RJ-J4NTM, bertsio guztiak.

Azalpena:

Trend Micro erakundeko TXOne IoT/ICS Security Research Labs taldeko Ta-Lun Yen ikertzaileak, Trend Microren Zero Day Initiative ekimenarekin elkarlanean, jakinarazi du legezko gailu baten ordezpen motako larritasun handiko ahultasun bat atzeman dutela. Mitsubishi Electric etxearen hainbat produkturi eragiten die.

Konponbidea:

Mitsubishi Electric konpainiak erabiltzaileei gomendatu die honako neurriak hartzeko, ahultasunak dakarren arriskua minimizatzeko:

- Segurtasun-gomendio orokorrak: firewall, VPN, LAN eta antibirus eguneratua erabiltzea.
- RnCPU (n = 00/01/02), 18 bertsioa eta aurrekoak: 19 edo osteko bertsioen arabera eguneratzea;
- RnCPU (n = 04/08/16/32/120), 50 bertsioa eta aurrekoak: 51 edo osteko bertsioen arabera eguneratzea;
- RnENCPU (n = 04/08/16/32/120), 50 bertsioa eta aurrekoak: 51 edo osteko bertsioen arabera eguneratzea;
- FX5U (C) - ** M * / **
-
    - 1. kasua: 17X *** serie zenbakia edo ostekoa, 1.210 bertsioa eta aurrekoa: 1.211 edo osteko bertsioen arabera eguneratzea;
    - 2. kasua: 179 *** serie zenbakia eta aurrekoa, 1.070 bertsioa eta aurrekoa: 1.071 edo osteko bertsioen arabera eguneratzea;
- FX5UC-32M * / ** - TS, 1.210 bertsioa eta aurrekoak: 1.211 edo osteko bertsioen arabera eguneratzea;
- FX5UJ - ** M * / **, 1.000 bertsioa: 1.001 bertsiora edo osteko batera eguneratzea.

Xehetasuna:

Baliteke erasotzaile batek gailuen ordeztea egitea kaltetutako produktuetan. Horren ondorioz, erasotzaile batek komando arbitrarioak exekutatu litzake urrutitik. Ahultasun horretarako, CVE-2020-16226 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Siemens segurtasun oharrak, 2020ko iraila

Argitalpen data: 2020/09/08

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Information Server, 2019 SP1 eta ostekoak;
- License Management Utility (LMU), V2.4 bertsioaren aurreko guztiak;
- Polarion Subversion Webclient, bertsio guztiak;
- Process Historian (Process Historian OPC UA Server barne), 2019 bertsioa eta ostekoak;
- SIMATIC Field PG M4, Field PG M5 eta Field PG M6, bertsio guztiak;
- SIMATIC HMI Basic Panels 2nd Generation (SIPLUS aldaerak barne), 14 bertsioa baino handiagoak edo berdinak eta XX bertsioaren aurrekoak;
- SIMATIC HMI Basic Panels 2nd Generation (SIPLUS aldaerak barne), bertsio guztiak;
- SIMATIC HMI Mobile Panels, bertsio guztiak;
- SIMATIC HMI United Comfort Panels, bertsio guztiak;
- SIMATIC IPC3000 SMART, IPC347E, IPC427D (SIPLUS aldaera guztiak), IPC427E (SIPLUS aldaerak barne), IPC477D, IPC477E, IPC477E Pro, IPC527G, IPC547E, IPC547G, IPC627D, IPC627E, IPC647D, IPC647E, IPC677D, IPC677E, IPC827D, PC847D, IPC847E, ITP1000, bertsio guztiak;
- SIMATIC PCS neo, bertsio guztiak;
- SIMATIC RTLS Locating Manager, V2.10.2 bertsioaren aurreko guztiak;
- SIMATIC S7-300 CPU family (ET200 CPUs eta SIPLUS aldaerak barne), bertsio guztiak;
- SIMATIC S7-400 CPU family (SIPLUS aldaerak barne), bertsio guztiak;
- SIMATIC WinCC OA, V3.17 bertsioa;
- SIMIT Simulation Platform, V10.0 bertsioa eta ostekoak;
- SIMOTION P320-4E eta P320-4S, bertsio guztiak;
- SINEC INS, bertsio guztiak;
- SINEMA Remote Connect, bertsio guztiak;
- SINUMERIK 828D (PPU.4 / PPU1740), SINUMERIK 840D sl (NCU730.3B), SINUMERIK ONE (NCU1750 / NCU1760);
- Siveillance Video Client, bertsio guztiak.
- Spectrum PowerTM 4, V4.70 SP8 bertsioaren aurreko guztiak;
- SPPA-S2000 (S7), V3.04 eta V3.06 bertsioak;
- SPPA-S3000, V3.04 eta V3.05 bertsioak;
- SPPA-T3000, R8.2 SP2 bertsioa;

Azalpena:

Siemensek produktu batzuen inguruan hainbat segurtasun-eguneratze argitaratu ditu, bere hileroko jakinarazpenean.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneratzeak Siemens deskarga paneletik deskargatu daitezke. Eguneratzerik gabeko produktuetarako, Erreferentzien atalean azaldutako arintze-neurriak aplikatu behar dira.

Xehetasuna

Siemensek, segurtasu: n partxeei buruzko hileroko jakinarazpenean, 19 segurtasun-abisu eman ditu; horietatik 10 eguneratzeak dira.

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- 1 vulnerabilidad de acceso al búfer con un valor de longitud incorrecta.
- Sarbide okerraren balioztatze motako ahultasun 1;
- Informazioa argitaratze motako ahultasun 1;
- Beharrezko pribilegiorik gabeko exekuzioaren ahultasun 1;
- Berez okerrak diren baimenen motako 2 ahultasun;
- Egiaztatze ezaren motako ahultasun 1;
- Baimen-emate okerren saiakeren mugatze desegokiaren motako ahultasun bat;
- Informazio sentikorra testu argi gisa gordetzearen motako ahultasun 1;
- Informazio sentikorra testu argi gisa transmititzearen ahultasun 1;
- Zifratze desegokiaren indarraren motako ahultasun 1;
- Jatorriaren balioztatze-akatsen motako ahultasun 1;
- Sinadura kriptografikoaren egiaztatze okerraren motako ahultasun 1;
- Leku gurutzatuetan eskaeraren faltsutze motako ahultasun 1 (Cross-Site Request Forgery);
- Baliabideak itzali edo liberazio okerra egitearen motako ahultasun 1;
- Komatxo artean sartu gabeko bilaketa-elementu edo ibilbidearen ahultasun 1;
- Behar ez bezala babestutako kredentzialen ahultasun 1;
- Informazioa direktorioen zerrendaren bidez erakusgai jartzearen ahultasun 1;
- Webgune bateko scriptekin erlazionatutako HTML etiketen neutralizazio desegokiari dagokion ahultasun 1 (XSS oinarrizkoa);
- Bufferrera luzera desegokia duen balio batekin sartzearen ahultasuna

Ahultasun horietarako, honako identifikatzaileak erreserbatu dira: CVE-2020-10049, CVE-2020-10050, CVE-2020-10051, CVE-2020-15791, CVE-2020-15788, CVE-2020-15789, CVE-2020-14509, CVE-2020-14513, CVE-2020-14515, CVE-2020-14517, CVE-2020-14519, CVE-2020-16233, CVE-2020-0543, CVE-2020-15786, CVE-2020-15787, CVE-2020-15784, CVE-2020-15790, CVE-2020-10056 eta CVE-2020-15785.

Etiketak: Eguneratzea, Siemens, Ahultasuna

Schneider erakundearen produktuen ahultasunak

Argitalpen data: 2020/09/09

Garrantzia: Handia

Kaltetutako baliabideak:

- SCADAPack 7x Remote Connect, V3.6.3.574 bertsioa eta aurrekoak;
- SCADAPack x70 Security Administrator, V1.2.0 bertsioa eta aurrekoak.

Azalpena:

Schneider Electric erakundeak hainbat ahultasunen berri eman du; 3 tarteko larritasunekoak eta 2 larritasun handikoak dira, eta SCADAPack 7x Remote Connect eta SCADAPack x70 Security Administrator produktuei eragiten diete. Kodearen exekuzio arbitrarioa ekar lezakete, babestu gabeko karpetetan edukia gehitu, edo kode exekutagarria duten karpetetan sartu.

Konponbidea:

SCADAPack 7x RemoteConnect V3.7.3.904 eta SCADAPack x70 Security Administrator V1.6.2 bertsioetara eguneratzea. Biak daude eskuragarri RemoteConnect V2.3.2 paketean.

Xehetasuna:

- Datu ez fidagarrien deserializazio arloko ahultasun baten ondorioz, kode arbitrarioa exekutatu liteke erasotzaile batek bereziki diseinatua dagoen PRJ artxibo bat eraikitzen duenean (buffer serializatu maltzur batekin). Tarteko larritasuna duen ahultasun horretarako CVE-2020-7528 identifikatzailea esleitu da.
- Direktorio mugatu baterako sarbide-ibilbide baten mugatze okerraren motako ("path transversal") ahultasun baten ondorioz, erasotzaile batek edukia jarri lezake sistemako babestu gabeko edozein karpetatan, bereziki diseinatutako .RCZ artxibo bat erabiliz. Tarteko larritasuna duen ahultasun horretarako CVE-2020-7529 identifikatzailea esleitu da.
- Baimen desegokiaren motako ahultasun baten bidez, erasotzaile bat kode exekutagarriaren karpetetara sar liteke. Larritasun handiko ahultasun horretarako CVE-2020-7530 identifikatzailea esleitu da.
- Sarbide kontrol desegokiaren arloko ahultasun baten bidez, erasotzaile batek exekutagarriak jar litzake karpeta espezifiko batean eta kodea exekutatu, betiere, erabiltzaileak RemoteConnect erabiltzen badu. Tarteko larritasuna duen ahultasun horretarako CVE-2020-7531 identifikatzailea esleitu da.
- Datu ez fidagarrien deserializazio arloko ahultasun baten ondorioz, kode arbitrarioa exekutatu liteke erasotzaile batek bereziki diseinatua dagoen .SDB artxibo bat eraikitzen duenean (buffer serializatu maltzur batekin). Larritasun handiko ahultasun horretarako CVE-2020-7532 identifikatzailea esleitu da.

Etiketak: Eguneraketa, Schneider Electric, Ahultasuna

Hainbat ahultasun AVEVA multinazionalaren Enterprise Data Management Web sisteman

Argitalpen data: 2020/09/09

Garrantzia: Handia

Kaltetutako baliabideak:

AVEVA Enterprise Data Management Web v2019 eta eDNAWeb gisa ezagunak diren aurreko bertsio guztiak.

Azalpena:

AVEVA enpresak SQL kodearen injekzio ahultasun batzuen berri eman du. Horien bidez, erasotzaile batek SQL komando arbitrarioak exekuta litzake.

Konponbidea:

AVEVATM Enterprise Data Management Web v2019 SP1 bertsiora eguneratzea; posible ez bada, laster jarriko da abian eDNAWebv2018SP2 bertsiorako hotfix bat.

Xehetasuna:

SQL komando batean (SQL injekzioa) erabilitako elementu berezien neutralizazio okerraren arloko hainbat ahultasun egonda, eDNAWeb sisteman erasotzaile batek SQL komandoak exekuta litzake, SQL sarbideetarako eDNA Web kontuaren pribilegioekin.

Etiketak: Eguneratzea, Ahultasuna

Hainbat ahultasun pazienteen monitorizaziorako Philips markako gailuetan

Argitalpen data: 2020/09/11

Garrantzia: Handia

Kaltetutako baliabideak:

- Patient Information Center iX (PICiX), B.02, C.02, C.03 bertsioak;
- PerformanceBridge Focal Point, A.01 bertsioa;
- IntelliVue patient monitors MX100, MX400-MX850 eta MP2-MP90, N bertsioa eta aurrekoak;
- IntelliVue X3 y X2, N bertsioa eta aurrekoak.

Azalpena:

Pazienteen monitorizaziorako Philips gailuetan hainbat ahultasun atzeman dira. Horien ondorioz, erasotzaile batek pazientearen datuak ikus litzake, aplikazioa berrabiarazi, ziurtagirien zerbitzua bat-batean itxi, sistema berrabiarazi, edo pribilegio batzuekin mugatutako eremutik irten.

Konponbidea:

Eguneratze hauek daude aurreikusita:

- Patient Information Center iX (PICiX) C.03 bertsioa, 2020ko amaierarako;
- PerformanceBridge Focal Point 2021eko bigarren lauhilekorako;
- IntelliVue Patient Monitors Versions N.00 and N.01 2021eko lehenengo lauhilekorako;
- IntelliVue Patient Monitors Version M.04 2021eko amaierarako;
- Ziurtagiriak indargabetzeko sistema 2023an ezarriko da.

Xehetasuna:

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Formula elementuen neutralizazio okerra CSV artxiboetan. Ahultasun horretarako, CVE-2020-16214 identifikatzailea esleitu da.
- Web orria sortu bitarteko sarreraren neutralizazio desegokia (Cross-site Scripting). Ahultasun horretarako, CVE-2020-16218 identifikatzailea esleitu da.
- Baimen-emate okerra. Ahultasun horretarako, CVE-2020-16222 identifikatzailea esleitu da.
- Ziurtagirien baliogabetzearen konprobazio okerra. Ahultasun horretarako, CVE-2020-16228 identifikatzailea esleitu da.
- Hutsaltasunaren erabilera desegokia parametroen luzeran. Ahultasun horretarako, CVE-2020-16224 identifikatzailea esleitu da.
- Sarrera-datuen zuzentzaile sintaktikoaren balioztatze desegokia. Ahultasun horretarako, CVE-2020-16220 identifikatzailea esleitu da.
- Sarrerako balioztatze okerra. Ahultasun horretarako, CVE-2020-16216 identifikatzailea esleitu da.
- Baliabidea kontrol-esfera oker batean erakusgai egotea. Ahultasun horretarako, CVE-2020-16212 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Osasuna, Ahultasuna

Ahultasuna FATEK Automation erakundearen PLC WinProladder baliabidean

Argitalpen data: 2020/09/11

Garrantzia: Handia

Kaltetutako baliabideak:

PLC WinProladder, 3.28 bertsioa eta aurrekoak.

Azalpena:

Hainbat ahultasun atzeman dira PLC WinProladde delakoetan, eta erasotzaile batek gailua kolapsatu lezake, zerbitzuaren ukapena egin, eta kodearen urrutiko exekuzioa burutu.

Konponbidea:

Harremanetan jartzea Fatek laguntza zerbitzuarekin.

Xehetasuna:

Pilan oinarritutako bufferraren gainezkatze motako ahultasuna baliatu lezake erasotzaileak, erabiltzaileren batek bereziki diseinatutako artxibo bat zabalduko balu. Horren ondorioz, kodearen urrutiko exekuzioa burutu liteke. Ahultasun horretarako, CVE-2020-10597 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun HiSilicon hardwarean oinarritutako IPTV kodegailuetan

Argitalpen data: 2020/09/16

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Ahultasun horiek kaltetutako fabrikatzaileak honakoak dira:

- URayTech;
- J-Tech Digital;
- VeCASTER PRO de Pro Video Instruments.

Beste marka batzuk oraindik ez dira konfirmatu.

Azalpena:

Hainbat ahultasun argitaratu dira (4 kritiko, handi bat eta ertain bat) HiSilicon Hi3520d hardwarean oinarritutako IP gaineko bideo-kodegailu batzuetan, IPTV/H.264/H.265 bideo-kodegailu izenez ere ezagunak. Ahultasun horiek baliatuta, baimenik gabeko urrutiko erasotzaile batek kode arbitrarioa exekuta lezake eta baimenik gabeko beste ekintza batzuk burutu, sistema ahul batean.

Konponbidea:

Fabrikatzailearen azken eguneratzeak aplikatzea. Informazio zehatzagoa izateko, kontsultatu erreferentzien atala.

Xehetasunak:

PTV/H.264/H.265 bideo-kodegailuen softwarean dauden ahultasunak honakoak dira:

- Administrazio-sarbide osoa atzeko ateko pasahitz baten bidez. Ahultasun horretarako, CVE-2020-24215 identifikatzailea erreserbatu da.
- Root administrazio sarbidea atzeko ateko pasahitz baten bidez. Ahultasun horretarako, CVE-2020-24218 identifikatzailea erreserbatu da.
- Zeharkako path bidez irakurritako artxibo arbitrarioa. Ahultasun horretarako, CVE-2020-24219 identifikatzailea erreserbatu da.
- Baimenik gabeko artxiboak igotzea. Ahultasun horretarako, CVE-2020-24217 identifikatzailea erreserbatu da.
- Kodearen exekuzio arbitrarioa, firmware maltzurraren bidez. Ahultasun horretarako, CVE-2020-24217 identifikatzailea erreserbatu da.
- Kode arbitrarioaren exekuzioa komando-injekzioaren bidez. Ahultasun horretarako, CVE-2020-24217 identifikatzailea erreserbatu da.
- Zerbitzu-ukapena bufferrak gainezka egitearen ondorioz. Ahultasun horretarako, CVE-2020-24214 identifikatzailea erreserbatu da.
- Bideo-emanaldira baimenik gabeko sarbidea RTSP bidez. Ahultasun horretarako, CVE-2020-24216 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Komunikazioak, IoT, Ahultasuna.

Hainbat ahultasun Advantech-en WebAccess Node sisteman

Argitalpen data: 2020/09/18

Garrantzia: Handia

Kaltetutako baliabideak:

WebAccess Node, 9.0.1 bertsioaren aurreko guztiak.

Azalpena:

Larritasun handiko ahultasun bat argitaratu da Advantech-en WebAccess Node sisteman. Horren ondorioz, erasotzaile batek pribilegioetan eskalatu lezake.

Konponbidea:

9.0.1 bertsiora eguneratzea.

Xehetasunak:

Kaltetutako produktuak ez dauka baimen egokirik zerbitzu espezifikoek erabilitako baliabideetarako, beraz, kodearen exekuzioa gerta liteke. Ahultasun horretarako, CVE-2020-16202 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun Wibu Systems enpresaren CodeMeter sisteman

Argitalpen data: 2020/09/18

Garrantzia: Kritikoa

Kaltetutako baliabideak:

CodeMeter Runtime tresnaren, lizentzia administratzailea, honako bertsioak kaltetu dira:

- 7.10a bertsioaren aurreko guztiak daude kaltetuta, CVE-2020-14509, CVE-2020-14517 eta CVE-2020-14519 bidez;
- 7.10 bertsioaren aurreko guztiak daude kaltetuta, CVE-2020-16233 bidez;
- 6.81 bertsioaren aurreko guztiak daude kaltetuta, CVE-2020-14513 bidez;
- 6.90 bertsioaren aurreko guztiak daude kaltetuta CVE-2020-14515 bidez, CmActLicense Firm Code duten CmActLicense eguneratze-artxiboak erabiltzen direnean.

Azalpena:

Claroty enpresako Sharon Brizinov eta Tal Keren ikertzaileek 6 ahultasunen berri eman dute; 2 larritasun kritikokoak eta 4 handikoak. Motak: bufferrera luzera-balioa ezegokiarekin sartzea, zifratze-indar desegokia, jatorri-balioztatze akatsa, sarrera-datuen balioztatze ez zuzena, sinadura kriptografikoaren egiaztatze desegokia eta baliabide desegokien liberazioa.

Konponbidea:

Wibu Systems-ek honako neurriak hartzea gomendatu da:

- CodeMeter Runtime azken bertsiora eguneratzea,
- CodeMeter Runtime soilik bezero gisa exekutatzea,
- API REST berria erabiltzea WebSockets sistemaren barneko APIaren ordez,
- WebSockets sistemaren APIa desgaitzea,
- AxProtector aplikatzea.

Ahultasun horien mende dauden fabrikatzaileek argitaratutako abisuen informazio zehatzagoa izateko, CISA abisuaren 5. *MITIGATIONS* atala kontsultatu..

Xehetasunak:

- Memoria ustelaren motako hainbat ahultasun daude. Horien bidez, paketeen analizatzaile mekanismoak ez ditu luzera-eremuak egiaztatzen. Erasotzaile batek paketeak bidal litzake, bereziki diseinatuak, ahultasun horiek baliatzeko. Ahultasun horretarako, CVE-2020-14509 identifikatzailea esleitu da.
- Protokoloaren zifratzea erraz urratu daiteke, eta zerbitzariak kanpo konexioak onartzen ditu. Hori horrela izanik, erasotzaile bat urrunetik jar daiteke harremanetan CodeMeter-en APIarekin. Ahultasun horretarako, CVE-2020-14517 identifikatzailea esleitu da.
- Ahultasun horren bidez, erasotzaile batek WebSockets-en barne APIa baliatu lezake, bereziki diseinatutako Java Script-en payload baten bidez, eta lizentzia-artxiboak sortu litezke, CVE-2020-14515 ahultasunarekin konbinatuta. Ahultasun horretarako CVE-2020-14519 identifikatzailea esleitu da.
- CodeMeter eta hori erabiltzen duen softwareak lizentzia-artxibo bat oker prozesatu lezakete, bereziki diseinatua, luzera-eremu ez egiaztatuak direla eta. Ahultasun horretarako, CVE-2020-14513 identifikatzailea esleitu da.
- Arazo bat dago lizentzia-artxiboaren sinaduraren egiaztatze-mekanismoan. Horren bidez, erasotzaileek lizentzia-artxibo arbitrarioak sor litzakete. Ahultasun horretarako, CVE-2020-14515 identifikatzailea esleitu da.
- Erasotzaile batek bereziki diseinatutako pakete bat bidal lezake, eta horren ondorioz zerbitzariak montikuluaren datuak dituzten paketeak itzuliko lituzke (heap). Ahultasun horretarako, CVE-2020-16233 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Siemens, Ahultasuna.

Hainbat ahultasun Philips Clinical Collaboration Platform sisteman

Argitalpen data: 2020/09/18

Garrantzia: Ertaina

Kaltetutako baliabideak:

Clinical Collaboration Platform 12.2.1 bertsioa eta aurrekoak.

Azalpena:

Northridge Hospital Medical Center zentroko ikertzaileek Clinical Collaboration Platform plataformaren hainbat ahultasunen berri eman dute. Horien bidez, erasotzaile batek zerbitzuaren ukapena eragin lezake (DoS), erabiltzaile bat engainatu eta Cross-site Request Forgery (CSRF) eraso bat burutu edo osteko beste eraso batzuetarako informazioa eman.

Konponbidea:

Clinical Collaboration Platform plataforma 12.2.5 bertsiora eguneratzea hainbat ahultasun konpontzeko, eta 12.2.1.5 partxea, gainerakoetarako. CVE-2020-16200 ahultasuna eskuz konpondu behar da.

Clinical Collaboration Platform plataformaren erabiltzaileak eskualde mailako laguntza zerbitzuarekin jar daitezke harremanetan, edo 1-877-328-2808 telefonora deitu.

Xehetasunak:

Clinical Collaboration Platform plataforman atzemandako ahultasun garrantzitsuenak honen ingurukoak dira: kontrol desegokia duen baliabide bat erakusgai geratzea, erasotzaileari baliabidera sartzeko informazioa emanez. Ahultasun honetarako CVE-2020-16247 identifikatzailea erreserbatu da.

Beste ahultasun garrantzitsuena baliabide mugatu baten kontrol-faltari dagokio. Horren ondorioz, erasotzaile batek kontsumitutako baliabideak aldatu litzake, eta zerbitzuaren ukapena egin. Ahultasun honetarako CVE-2020-16200 identifikatzailea erreserbatu da.

Beste ahultasun batzuetarako CVE-2020-16198, CVE-2020-14525 eta CVE-2020-14506 identifikatzaileak erreserbatu dira.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, Pribatutasuna, Osasuna, Ahultasuna.

Hainbat ahultasun MB connect line produktu batzuetan

Argitalpen data: 2020/09/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- mymbCONNECT24, v2.6.1 bertsioa eta aurrekoak;
- mbCONNECT24, v2.6.1 bertsioa eta aurrekoak;

Azalpena:

 plataformak OTORIOk MB connect line-ri jakinarazitako ahultasunak koordinatu ditu. Horrela izanik, erasotzaile batek informazioa zabal lezake.

Konponbidea:

Kaltetutako produktuak v2.6.1. bertsioaren osteko bertsio batera eguneratzea.

Xehetasunak:

- Knximport eta lancompenent sistemen SQL injekzioko ahultasun baten bidez, baimendutako erasotzaile batek informazio arbitrarioa antzeman lezake. Ahultasun horietarako CVE-2020-24569 eta CVE-2020-24568 identifikatzaileak erreserbatu dira.
- Server-Side Request Forgery (SSRF) eta Cross-Site Request Forgery (CSRF) motako ahultasunaren bidez, erasotzaile batek saioko informazioa lapurtu lezake, bereziki diseinatutako loturen bidez. Ahultasun horretarako, CVE-2020-24570 identifikatzailea esleitu da.
- Hirugarrenen software zaharkitu eta erabili gabea erabiliz, kodearen urrutiko exekuzioa gerta liteke, ustiapen kate baten bidez.

Etiketak: Eguneratzea, Birtualizazioa, Ahultasuna

Hainbat ahultasun General Electric etxearen produktu batzuetan

Argitalpen data: 2020/09/23

Garrantzia: Altua

Kaltetutako baliabideak:

- GE Digital APM Classic, 4.4 bertsioa eta aurrekoak;
- GE Reason S20 Ethernet Switch, bertsioak:
  - S2020, 07A06 bertsioaren aurreko firmware bertsio guztiak;
  - S2024, 07A06 bertsioaren aurreko firmware bertsio guztiak;

Azalpena:

Guido Marilli, Accenture Security erakundeko ikertzaileak, eta IOActive konpainiak 4 ahultasunen berri eman diote GE enpresari; 2 larritasun handikoak eta 2 ertainekoak. Motak: erabiltzaileak kontrolatutako gakoaren bidezko baimen-omisioa, salt gabeko norabide bakarreko hash erabiltzea eta XSS.

Konponbidea:

- GE Digital APM Classic 4.5 bertsiora edo goragokoetara eguneratzea, GE Digitaleko ordezkari batekin kontaktatuz;
- GE Reason S20 Ethernet Switch 07A06 edo osteko firmware bertsio batera eguneratzea.

Xehetasunak:

- IDOR (Insecure Direct Object Reference) ahultasun baten bidez, erasotzaile batek erabiltzaile kontuekin erlazionatutako datu konfidentzialak deskargatu litzake, pribilegio egokirik izan gabe. Ahultasun horretarako, CVE-2020-16240 identifikatzailea esleitu da.
- Salt (datuen hash, pasahitza edo pasahitz-esaldia erabiltzen duen norabide bakarreko funtzio baterako sarbide gehigarri moduan erabilitako datu aleatorioak) ez da erabiltzen pasahitzen hash delakoa kalkulatzeko, horrela deszifratzea lor daitekeelako, plataforma osoa arriskuan jarriz; izan ere, baimendutako erabiltzaile batek erabiltzailearen kontuaren datu guztiak berreskura litzake, eta gero pasahitz errealak lortu. Ahultasun horretarako, CVE-2020-16244 identifikatzailea esleitu da.
- Kaltetutako produktua XSS (Cross-Site Scripting) ahultasunaren mende egon daiteke. Horrela, erasotzaile batek erabiltzaileak engaina litzake ekintza kritikoak burutzeko. Horien artean daude, esaterako, kontuak gehitu eta eguneratzea. Ahultasun horretarako, CVE-2020-16242 identifikatzailea esleitu da.
- Kaltetutako produktua XSS ahultasunaren mende egon daiteke. Horrela izanik, erasotzaileek erabiltzaileak engainatu litzakete lotura bati jarraitzeko edo JavaScript kode maltzurra duen orri batera nabigatzeko. Horrela, biktimak kode hori prozesatu eta exekutatu egingo luke. Ahultasun horretarako, CVE-2020-16246 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

DLL bahiketa arloko ahultasuna Eaton 9000x sisteman

Argitalpen data: 2020/09/28

Garrantzia: Altua

Kaltetutako baliabideak:

Eaton markaren 9000x programazio eta konfigurazio softwarea, 2.0.38 bertsioa eta aurrekoak..

Azalpena:

Yongjun liu ikertzaileak larritasun handiko ahultasun baten berri eman du, DLL bahiketa arlokoa (DLL hijacking).

Konponbidea:

Produktua eguneratzea 2.0.41 bertsiora.

Xehetasunak:

Erasotzaile batek kode arbitrarioa exekuta lezake, vci11un6.DLL eta cinpl.DLL ordeztuz aplikazioak DLLak kargatu nahi dituenean eragiketa normalak egiteko. Ahultasun horretarako, CVE-2020-6654 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun B&R Industrial Automation produktu batzuetan

Argitalpen data: 2020/09/30

Garrantzia: Altua

Kaltetutako baliabideak:

- SiteManager, 9.2.620236042 bertsioaren aurreko guztiak;
- GateManager 4260 eta 9250, 9.0.20262 bertsioaren aurreko guztiak;
- GateManager 8250, 9.2.620236042 bertsioaren aurreko guztiak.

Azalpena:

Nikolay Sokolik eta Hay Mizrachi ikertzaileek 6 ahultasunen berri eman dute; 2 larritasun handikoak dira, eta beste 4 tarteko larritasunekoak. Motak: direktorio mugatu baterako sarbidea (path transversal), kontrolik gabeko baliabide-kontsumoa, informazioa erakusgai jartzea, eta baimen desegokia.

Konponbidea:

B&R Industrial Automation etxeak jakinarazi du ahultasunak honako bertsioetan konpondu direla:

- SiteManager: 9.2.620236042;
- GateManager 4260 y 9250: 9.0.20262;
- GateManager 8250: 9.2.620236042.

Xehetasunak:

- Baimena lortzen duen erasotzaile batek zerbitzuaren konfigurazioa eta bestelako informazio konfidentzialen bat irakur lezake, eta SiteManager sistemako instantzietan jarduera maltzurretarako erabili. Ahultasun horretarako, CVE-2020-11641 identifikatzailea esleitu da.
- Erasotzaile batek SiteManager instantzien etengabeko berrabiarazte bat eragin lezake, eta horrek eskuragarritasuna mugatuko luke. Ahultasun horretarako, CVE-2020-11642 identifikatzailea esleitu da.
- Erasotzaile batek atzerriko erakunde baten jabetzakoak diren gailuei buruzko informazioa bildu lezake, eta informazio hori jarduera maltzurretarako erabili. Ahultasun horretarako, CVE-2020-11643 identifikatzailea esleitu da.
- Baimena lortzen duen erasotzaile batek atzerritar domeinuen erabiltzaileak engainatu litzake ikuskaritza faltsuen inguruko alerta edo mezuekin. Ahultasun horretarako, CVE-2020-11644 identifikatzailea esleitu da.
- Baimena lortzen duen erasotzaile batek GateManager instantziak berrabiaraz litzake behin eta berriro, eta horrek eskuragarritasuna mugatuko luke. Ahultasun horretarako, CVE-2020-11645 identifikatzailea esleitu da.
- Baimena lortzen duen erasotzaile batek domeinuaren barruko gailu guztien informazioa lortu lezake, eta informazio hori jarduera maltzurretarako erabili. Ahultasun horretarako, CVE-2020-11646 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, Ahultasuna.

Kontrolik gabeko kontsumoa Mitsubishi Electric MELSEC iQ-R Series baliabideetan

Argitalpen data: 2020/09/10

Garrantzia: Altua

Kaltetutako baliabideak:

MELSEC iQ-R modulu hauek daude kaltetuta:

- R00 / 01 / 02CPU, bertsio guztiak,
- CPU R04 / 08/16/32/120 (EN), bertsio guztiak,
- R08 / 16/32 / 120SFCPU, bertsio guztiak,
- R08 / 16/32 / 120PCPU, bertsio guztiak,
- R16 / 32 / 64MTCPU, bertsio guztiak.

Azalpena:

SCADAfence erakundeko Yossi Reuven ikertzaileak ahultasun bat atzeman du Mitsubishi Electric markako MELSEC iQ-R seriean. Horren ondorioz, zerbitzu-ukapen bat gerta liteke, kontrolik gabeko erabileragatik.

Konponbidea:

Mitsubishi Electricek partxe bat argitaratuko du laster, ahultasun horretarako. Galderarik baduzu, kontsultatu Mitsubishi Electriceko ordezkariren batekin.

Mitsubishi Electricek erabiltzaileei gomendatu die arriskua murrizteko honako neurriak hartzeko:

- Sare pribatu birtual bat erabiltzea (VPN), Internet bidezko baimenik gabeko sarbidea saihesteko.
- Gailuaren arrisku-aukerak minimizatzea, LAN sarerako sarbidez murriztu eta konfiantzazkoak ez diren ekipoetarako sarbidea blokeatzea, suebakien bidez.

Xehetasunak:

Antzemandako ahultasuna urrutitik baliatu liteke, bereziki diseinatutako paketeak bidaliz MELSEC iQ-R serieko moduluetara, baliabideen kontsumo kontrolik gabea eta zerbitzu ukapena eraginez.

Ahultasun horretarako, CVE-2020-16850 identifikatzailea esleitu da.

Etiketak: Azpiegitura kritikoak, SCADA, Ahultasuna.