SCHNEIDER ELECTRIC'S MODICON M221 PLC-EN AHULTASUNAK

BCSC_ALERTA_AHULTASUNAK_
SCHNEIDER_ELECTRIC_ MODICON_M221

TLP:WHITE

www.basquecybersecurity.eus

2020ko Azaroa

AURKIBIDEA

Erantzukizunetik salbuesteari buruzko klausula

Honako dokumentu hau eskaintzen da erakundeen eta interesa duten herritarren segurtasunerako BCSCk beharrezkotzat jotzen dituen alertak ezagutzera emateko. Inongo kasutan BCSC ezin da kontsideratu hemen zabaldutako informazioaren erabilpenak zuzenean nahiz zeharka, ustekabean nahiz modu berezian, eragin litzakeen balizko kalteen arduradun. Gauza bera esan beharra dago BCSCren webean edo hortik esteken bitartez joan litekeen kanpoko web orrialdeetan, sare sozialetan, software produktuetan edo alertan nahiz BCSCren webean agertutako beste edozein informaziotan aipa litezkeen teknologiei dagokienez. Edozein kasutan, alertaren edukiak eta mezu elektronikoen bidez eman litezkeen erantzunak hemen jasotako terminoetan emandako iritzi eta gomendioak dira eta jakinarazitako informaziotik ezin da ondorioztatu ondorio juridiko loteslerik.

Salmenta debekatzeari buruzko klausula

BCSC-RI BURUZ

Zibersegurtasun Euskal Zentroa (Basque Cybersecurity Centre, BCSC) da Eusko Jaurlaritzak izendatutako entitatea Euskadin zibersegurtasunaren gaian heldutasun maila igotzeko.

Zeharkako ekimena da, Enpresa Garapenerako Euskal Agentziaren (SPRI) barnean kokatua, Eusko Jaurlaritzako Ekonomiaren Garapen eta Azpiegitura Sailaren menpe dagoen sozietatea. Era berean, Eusko Jaurlaritzako beste hiru Sail ere inplikatzen ditu: Segurtasuna, Gobernantza Publiko eta Autogobernua, eta Hezkuntza; bai eta Zientzia, Teknologia eta Berrikuntzako Euskal Sistemako lau eragile ere: Tecnalia, Vicomtech, Ikerlan eta BCAM.

BCSC erreferentziazko entitatea da zibersegurtasuna eta konfiantza digitala garatzeko Euskadiko herritar, enpresa eta instituzio publikoen artean, eta batez ere, eskualdeko ekonomiaren sektore estrategikoen kasuan.

Beraz, BCSCren eginkizuna da euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa jarduera dinamizatzea, eta erreferentzia izango den sektore profesional bat sor dadin eragitea. Testuinguru horretan osagarriak diren eragileen arteko lankidetza proiektuak exekutatzea sustatzen du, berrikuntza teknologikoaren, ikerkuntzaren, eta fabrikazio aurreratuko industriarako eta beste sektore batzuetarako transferentzia teknologikoaren alorretan.

Era berean, hainbat zerbitzu eskaintzen ditu Gertakarien Aurreko Ekipo modura duen rolagatik (aurrerantzean CERT, ingelesezko izenaren siglak direla-eta “Computer Emergency Response Team”). Euskal Autonomia Erkidegoko esparruan mehatxu berriak antzemateko eta horiei buruzko alerta goiztiarrak emateko gaitasuna areagotzen dihardu lanean, informazioaren segurtasun gertakarien erantzunean eta analisian, eta euskal gizartearen beharrak artatzeko beharrezkoak diren prebentzio neurrien diseinuan. Helburu horiek lortzeko xedearekin, zibersegurtasun gertakariak kudeatzera zuzendutako hainbat ekimenetan hartzen du parte:

LABURPEN EXEKUTIBOA

Schneider Electric-en Modicon M221 kontrolatzaile logiko programagarrien gama (PLC) asko erabiltzen da industria-sektoreko makinak automatizatzeko. Hainbat ahultasun ditu, eta horiek kautotu gabeko erasotzaile batek ustia ditzake OT sarerako sarbidearekin, M2Basure gailuaren eta EcoStruxure Machine Expert Basic softwarearen artean datu-trafikoan erabilitako **zifratua hausteko gailuaren kontrol osoarekin.**

Bestalde, Schneider Electric-ek **gomendio** eta **arintze-neurri** batzuk argitaratu ditu, gerta daitezkeen erasoen eragina murrizteko; izan ere, oraingoz ez da aurreikusten akatsak konpontzeko segurtasun-eguneratzerik.

AZTERKETA TEKNIKOA

Schneider Electric-en kontrolatzaile logiko programagarrien (**PLC**) **Modicon M221** gaman lau ahultasun daudela jakinarazi dute segurtasun-ikertzaileek. Errendimendu handiko gailuak dira, eta industria-sektorean asko erabiltzen dira makinen automatizazioa modu intuitibo eta malguan kontrolatzeko, eraginkortasuna hobetuz.

Ahultasunek gailu zaurgarrietan aldaketak egiteko aukera eman diezaiokete baimenik gabeko erabiltzaile bati, hainbat erasoren bidez: autentifikazioa saihestea, datuak transferitzeko erabilitako zifratua haustea eta komandoak exekutatzea. Horri esker, kontrolatzaileen kontrol osoa lortuko luke.

Hala ere, lehen aipatutako aldaketak egiteko, erasotzaile batek aldez aurretik OT sareko azpiegituran presentzia izan beharko luke, eta trafikoa atzeman EcoStruxure Machine ExpertBasic softwarearen eta Modicon M221 delakoaren PLC gailuen artean, ahultasunen ustiapena XOR zifratze-algoritmo ahul baten inplementazioan oinarritzen baita nagusiki.

Ondoren, identifikatutako ahultasunak deskribatzen dira:

- **CVE-2020-7565**. Datuak zifratzeko erabiltzen den 4 byteko XOR zifratze-giltza ezartzeak eragiten du zaurgarritasuna; izan ere, ez da behar bezain sendoa, eta, horri esker, erasotzaile batek idazketa- eta irakurketa-zifratzearen gakoa hautsi eta EcoStruxure Machineren softwarearen eta Modicon kontrolatzailearen arteko trafikoa atzeman dezake. Horretarako, erasotzaile batek testu plano ezaguneko erasoak erabili beharko lituzke, hau da, ezagutzen diren memoria-sekzioak eta dagoeneko zifratuta dauden homologoak alderatu beharko lituzke, edo trafikoan XOR gakoen sekuentzia errepikakorren analisi estatistikoa egin.
- **CVE-2020-7566**. Modicon M221 gailuek fitxategi ahulak trukatzeko ezarpen kriptografiko bat erabiltzen dute. Ezarpen horren bidez, Diffie-Hellman gakoak trukatzeko metodoa erabiltzen da 4 byteko XOR gako bat sortzeko. Hala, erasotzaile batek datuen transferentziarako erabilitako gakoa ondoriozta dezake, indar gordineko eraso baten bidez.
- **CVE-2020-7567**. EcoStruxure Machineren softwarearen eta Modicon kontrolatzaileen arteko komunikazioak 4 byteko XOR zifratuaren bidez babestuta daude. Beraz, enkriptatze-gakoa ondorioztatzea lortzen duen erasotzaile batek gako hori erabil dezake datuak transferitzeko pasahitzaren hash-a jakiteko eta *Pass-the-Hash* gailua izeneko alboko mugimenduko erasoa erabiltzeko.
- **CVE-2020-7568**. Memoria atal batzuetan ez da pasahitzik eskatzen, ezta irakurketa eta idazketa babesak aktibatuta badaude ere. Horri esker, erasotzaile batek informazio mugatua eskuratu dezake.

Oraingoz, **NIST**ren datu-baseak ez du ahultasun horietako bakar bat ere erregistratu, nahiz eta Schneider Electric-ek argitaratutako oharrean **7.1** puntuazioa eman dien ahultasunei, **CVSSv3** eskalaren arabera.

Orain arte, ez dakigu sareko ahultasun horien ustiapen aktiboari buruz, ez eta akatsak aprobetxatzeko publikoki eskuragarri dauden kontzeptu-probei buruz ere.

Schneider Electric-ek baieztatu du kontrolatzaile logiko programagarrien (PLC) **Modicon M221** gamako **bertsio guztiek** ahultasun horien eragina dutela.

ARINTZEA / KONPONBIDEA

Schneider Electric-ek argitaratutako segurtasun-oharrean, akatsak konpontzeko eguneraketarik ez dagoenez, horrek zenbait **arintze-neurri** hartu ditu, erasoen arriskua murrizteko. Fabrikatzaileak deskribatu dituen arintze-neurriak hauek dira:

- **Sarea segmentatzea** eta **firewall** bat ezartzea, TCP **502** porturako baimendu gabeko sarbide guztiak blokeatzeko.
- **Erabili gabeko protokolo** guztiak **desgaitzea**, bereziki **programazio**-protokoloa, programazioaren funtzionalitatea nahi gabe urrutitik eskuratu ez dadin.

Neurri hori gauzatzeko, EcoStruxure Machine Expert- PLC M221erako lineako oinarrizko laguntza gidako “Ethernet sarearen konfigurazioa” atala kontsultatzea gomendatzen da.

- Honakoetarako pasahitz segurua ezartzea:
  - Azpiegitura babestea.
  - Gailuan irakurtzeko sarbidea murriztea.
  - Gailuan idazteko sarrera murriztea.

Garrantzitsua da pasahitz desberdinak ezartzea lehen azaldutako helburu bakoitzerako.

Horrez gain, enpresak zerrenda bat eskaini du industria-eremuari aplikatutako zibersegurtasuneko **jardunbide egokiekin**:

- Industria kontrol eta segurtasuneko sistemen sareak firewall-aren bidez babestea eta empresa sareko gainerakoetatik isolatzea.
- Baimenik gabeko langileak kontrol eta segurtasun industrialeko sistemetara sar daitezen eragoztea.
- Ez konektatu programazio-softwarea horretarako ez den beste sare batera.
- Sare isolatuarekin datuak trukatzeko metodo guztiak eskaneatzea terminaletan edo kontrol eta segurtasun industrialeko sistemen sareetara konektatutako edozein nodotan erabili aurretik.
- Kontrol eta segurtasun industrialeko sistemen esposizioa murriztea, Internetetik irisgarriak ez direla ziurtatuz.
- VPN bezalako urruneko sarbide-metodo seguruak erabiltzea.

ERREFERENTZIA OSAGARRIAK

- Schneider Electric Security Notification - Modicon M221 Programmable Logic Controller
- Claroty, Schneider Electric disclose Modicon M221 authentication bypass flaws

Gertakarien jakinarazpena

Zibersegurtasun gertakariren bat aurkitu baduzu jakinaraz iezaguzu, horrela beharrezkoak diren neurriak hartuko ditugu zabal ez dadin.

900 104 891

arazoak@bcsc.eus

Zibersegurtasun katalogoa

Zure zibersegurtasunarekin edo zure enpresarenarekin laguntza behar duzu?