Ahultasunak TBox-en RTU gailuetan

BCSC-AHULTASUN-RTU-TBox

TLP:WHITE

www.basquecybersecurity.eus

2021eko Martxoa

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

Guztiz debekatuta dago dokumentu hau saltzea edo beragatik edozein onura ekonomiko eskuratzea, baina posible da bera kopiatzea, banatzea, hedatzea edo ezagutzera ematea.

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, Jasangarritasun eta Ingurumen Sailaren menpe dagoen sozietatea. Era berean, Eusko Jaurlaritzako beste hiru Sail ere bere parte dira: 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.

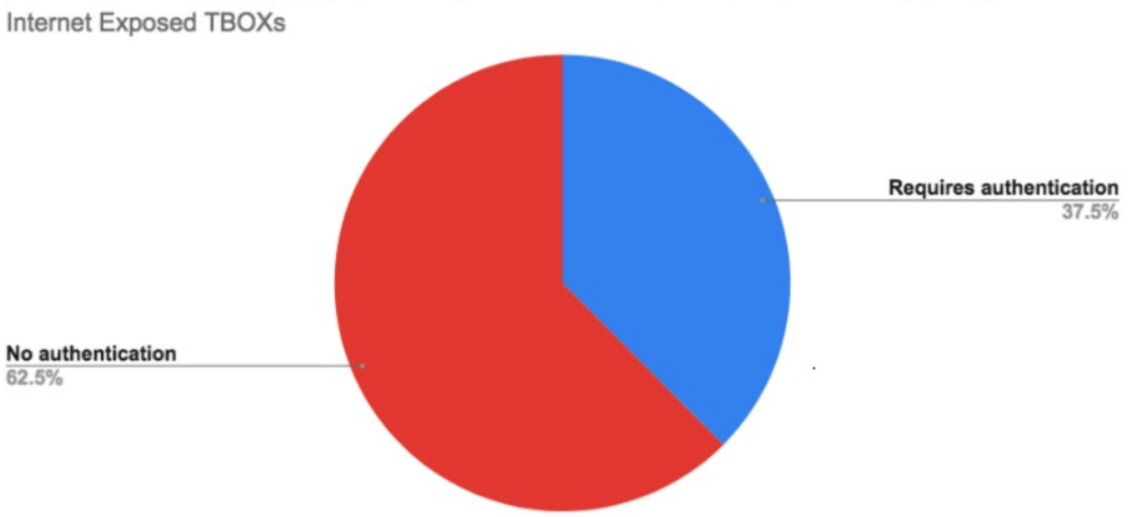
Beraz, BCSCren eginkizuna da euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa jarduera dinamizatzea, eta erreferentzia izango den sektore profesional bat sor dadin eragitea. Testuinguru horretan osagarriak diren eragileen arteko lankidetza proiektuak exekutatzea sustatzen du, 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, ingeleseko 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:

1. LABURPEN EXEKUTIBOA

Azpiegitura kritikoko osagaiak Internetera konektatzeak beti dakar enpresek kontuan hartu beharreko arriskuak. Batzuetan, konfiantza handiegia izaten da konfigurazio lehenetsietan. Konfigurazio horiek ez dira beti egokienak izaten, eta gainera, ez zaie kasurik egiten identifikatzen dituzten ahultasunei buruz ohartarazten duten ikertzaileei. Izan ere, ahultasun horietako asko gaizki konfiguratutako web-interfazeen azalpenarekin, kautotzeko mekanismorik ezarekin edo sistema kritikoak monitorizatzeko permisibitatearekin lotuta daude.

Horren adierazgarri da Claroty zibersegurtasunean espezializatutako enpresako adituek argitaratutako azken ikerketa. Duela gutxi argitaratutako oharraren arabera, Ovarro fabrikatzailearen TBX urruneko unitate terminalei (RTU) eragiten dieten zenbait ahultasun hauteman dira. Konpainia eta haren RTU TBox asko erabiltzen da azpiegitura kritikoetan, bereziki energia-, petrolio-, gas- eta garraio-industrietan. Internetera konektatutako TBox RTU guztien %37k bakarrik du gailua erasoetatik babesteko kautotze-motaren bat.



1. irudia: TBox gailuak, autentifikaziorik gabe/autentifikazioarekin.

Hutsegite horiek gailuetako segurtasun-politikak saihesteko erabil daitezke, gailuetara pribilegio handiekin iristeko, zerbitzua ukatzeko (DoS) eraso bat eragiteko edo kodea urrunetik exekutatzeko. TBox modelo guztiei eragiten die, baita TWinSoft 12.4 baino lehenagoko bertsio guztiei ere.

Ovarro konpainiak adierazi du TBox firmwarearen 1.46 bertsioan eta TWinSOft 12.4 bertsioan zuzendu direla Clarotyk emandako ahultasun guztiak. Beraz, erabiltzaile guztiei ahalik eta azkarren eguneratzea gomendatzen zaie.

2. AZTERKETA TEKNIKOA

Clarotyko ikertzaileek ahultasun horiek identifikatu dituzte Modbus protokoloaren Ovarroren bertsio patentatuaren inplementazioetan. Protokolo hori OSI ereduaren 1, 2 eta 7. mailetan dago kokatuta, eta bezeroaren/zerbitzariaren arkitekturan oinarritzen da. Protokolo honetan emandako akatsei esker, eguneratze-paketeak aldatu eta horietan kode maltzurra sar daiteke. Guztira, bost ahultasun aztertu dira. Hona hemen xehetasun tekniko ezagunak, eta fabrikatzaileak jakinarazi dituenak.

- CVE-2021-22640: Kredentzialak babesteko segurtasun-politikak behar bezala baliozkotzen ez direnez, erasotzaileek saio-hasierako pasahitza deszifratu dezakete, komunikazioak edo indar gordineko erasoak atzemanez. Informazio osagarria duen ohar hau argitaratu du enpresak.

- CVE-2021-22642**:** Ahultasuna, barne-baliabideen kontsumoaren kontrol ez-eraginkorraz baliatzen dena, erasotzaileei zerbitzua ukatzeko erasoak (DoS) eragiteko bereziki diseinatutako Modbus sareak erabiltzeko aukera ematen diena. Informazio osagarria duen ohar hau argitaratu du enpresak.

- CVE-2021-22644**:** Kodetutako gako batekin "TWinSoft" erabiltzaile pertsonalizatua erabiltzean TWinSoft-en akats gisa erabiltzen den ahultasuna. Akats horri esker, informazio sentikorra lor daiteke, eta horrela, kaltetutako sistemaren osotasuna arriskuan jartzen da. Informazio osagarria duen ohar hau argitaratu du enpresak.

- CVE-2021-22646**:** Sarrera-baliozkotze desegoki bat ipk paketeetan baliatzen duen ahultasuna. Modbus protokoloak eguneraketak ezartzen ditu mota horretako paketeen bidez. Pakete horiek aldi baterako fitxategi batean kargatzen dira, ipk fitxategiaren izena duen eguneratze-komando bat RTUra bidali aurretik, eta hor direktorio batera ateratzen da. Akats horrek aukera ematen du eguneratze-paketearen fitxategia HHSra bidali aurretik aldatzeko; beraz, exekutagarri maltzurrak sar daitezke, edo urruneko kode bat exekutatzeko aukera eman. Informazio osagarria duen ohar hau argitaratu du enpresak.

  CVE-2021-22648**:** Baliabide kritikoetarako baimenak oker esleitzeaz baliatzen den ahultasuna, Modbus artxibora sartzeko funtzioen barruan. Akats horrek konfigurazio-fitxategiak irakurri, aldatu edo ezabatzeko aukera ematen du. Informazio osagarria duen ohar hau argitaratu du enpresak.

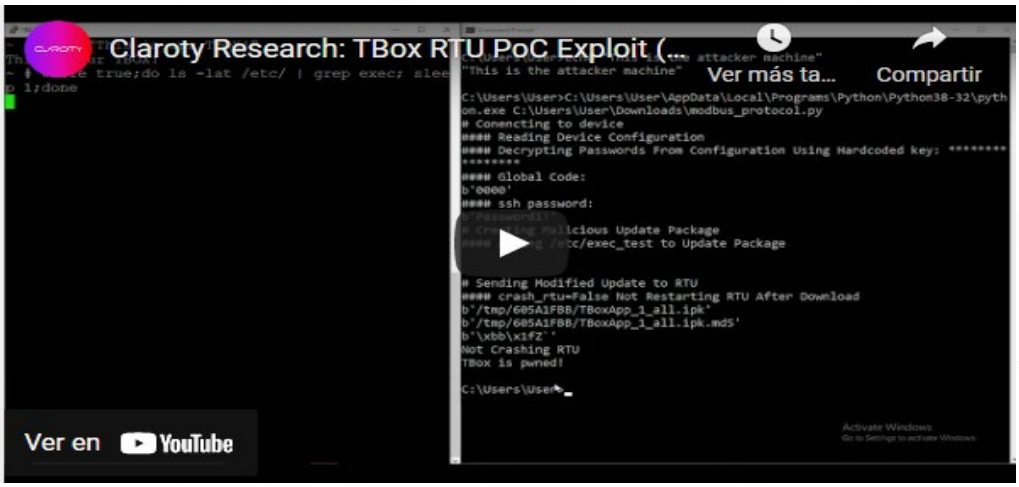
Ahultasun horiek produktu hauei eragiten diete:

- TBoxLT2 (eredu guztiak).
- TBox MS-CPU32.
- TBox MS-CPU32-S2.
- TBox MS-RM2 (eredu guztiak).
- TBox TG2 (eredu guztiak).
- TWinSoft 12.4 baino lehenagoko bertsio guztiak eta TBox Firmware 1.46 baino lehenagokoak.

NISTren datu baseak ez ditu oraingoz ahultasunak erregistratu; beraz, ez dute CVSSv3 eskalaren araberako puntuaziorik jaso. Hala ere, akats horiek aurkitu dituzten ikertzaileen arabera, eta konpainiak berak onartu duenez, ahultasun horiek kritikotzat jo dira, kodea urrunetik exekutatzeko, sareko trafikoa atzemateko eta zerbitzua ukatzeko erasoak eragiteko aukera ematen baitute. Gaur egun ez dakigu ahultasunak aktiboki ustiatzen ari diren, ez eta horretarako bide ematen duten ustiapenak dauden ere.

Ahultasun horien berri eman zuten ikertzaileek bideo bat argitaratu dute. Bideo horretan, kontzeptu-proba bat (PoC) azaltzen da, eta akats horiek ustiatzeko eman dituzten pausoak zehazten dira. Bideoan hiru ahultasun ageri dira (CVE-2021-22644, CVE-2021-22646 eta CVE-2021-22648), babestutako TBox batean kodea exekutatzeko kateatuta. Hona hemen eman beharreko pausoak:

- Konfigurazio fitxategia gailutik irakurtzea, MODBUS protokoloa erabiliz.
- Zifratutako pasahitzak ateratzea. Kodetutako gako bat erabiliz deszifratzen dira.
  Deskarga ezazu */etc/exec_test-en* fitxategi exekutagarri bat duen eguneratze maltzurreko pakete bat RTUan.



2. irudia: PoC CVE-2021-22644, CVE-2021-22646 eta CVE-2021-22648.

3. ARINTZEA / KONPONBIDEA

Ahultasunak TWinSoft-en 12.4 bertsioan eta TBox-en firmwarearen 1.46 bertsioan jaso dira. Azken bertsioak fabrikatzailearen web orrian daude, bezeroaren arretarako atalean (zerbitzuaren atarian).

Bestalde, CISAk gomendatzen du gailu horiek Interneten ahalik eta gutxien egotea, sare eta gailuak sare komertzialen kontrol-sistematik isolatzea eta urruneko sarbiderako VPN erabiltzea. Erabiltzaileei eskatzen zaie babes-neurri horiek har ditzatela ahultasun horiek ustiatzeko arriskua minimizatzeko:

- Sarearen esposizioa minimizatzea kontrol-sistemako gailu eta/edo sistema guztientzat, eta Internetetik eskuragarriak ez direla ziurtatzea.
- Kontrol-sistemaren sareak eta urruneko gailuak Firewall-en atzean kokatzea eta gailu horiek enpresa-saretik isolatzea.
- Urruneko sarbidea behar denean, metodo seguruak erabili, hala nola sare pribatu birtualak (VPN). VPNek ahultasunak izan ditzakete, eta bertsio berrienera eguneratu behar dira.

4. ERREFERENTZIA OSAGARRIAK

- Claroty Uncovers Vulnerabilities in TBox RTUs
- ICS Advisory (ICSA-21-054-04)
- Vulnerabilities in TBox RTUs Can Expose Industrial Organizations to Remote Attacks
- Multiple vulnerabilities in Ovarro TBox

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?