499ES ETHERNET/RTA-REN IP STACK-EN AHULTASUNA

BCSC_ALERTA_AHULTASUNAK_
499ES_ETHERNET/RTA-REN_IP_STACK-EN

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

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 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

Segurtasun-ikertzaileek adierazi dute **Real Time Automation-ek (RTA)** garatutako **499ES EtherNet/IP (ENIP) stack-en** ezarpenetan **ahultasun larria** dagoela, automatizazio industrialeko hainbat gailutan baitaude.

CVE-2020-25159 ahultasuna buffer-gainezkatze batean oinarritzen da. Gainezkatze horrek aukera eman diezaioke kautotu gabeko urruneko erasotzaile bati zerbitzua ukatzeko (**DoS**) eta kodea (**RCE**) exekutatzeko.

Zehazki, akatsa **2.28 baino lehenagoko bertsio** guztietan dago, EtherNet/IPren (ENIP) stack eskualdeko iturburu-kodean sartu gabe. Kode hori Real Time Automation-ek ordeztu zuen 2012an, nahiz eta hirugarrenen hainbat firmwarretan oraindik erabiltzen jarraitzen den. Ikertzaileen arabera, Internetera konektatutako 8.000 gailu baino gehiago bateragarriak dira ENIPrekin.

Ahultasuna konpontzeko, kaltetutako produktuaren azken bertsioa **eguneratu** behar da, Real Time Automation ekipoarekin harremanetan jarrita.

AZTERKETA TEKNIKOA

499ES EtherNet/IP (ENIP) memoriako stackaren iturburu-kodeak, Real Time Automation-ek (RTA) garatuak eta automatizazio industrialeko hainbat gailutan erabiliak, zaurgarritasun bat du, eta industria askok urruneko erasoak jasan ditzakete.

Kontrol eta Informazio estandarrean (CIP) oinarritutako EtherNet/IP (**ENIP**) sare-protokoloa asko erabiltzen da automatizazio industrialeko aplikazioetan, gailuen arteko komunikazioa denbora errealean egokia dela bermatzeko.

Arazoa da fabrikatzaile askok erabiltzen dituztela beren gailuetan hirugarrenek garatutako protokolo honen inplementazioak. Kasu honetan, Real Time Automation-ek garatutako inplementazioa da, zehazki, 2012 baino lehenagoko 499ES EtherNet/IP (ENIP) bertsioak.

CVE-2020-25159 erreferentzia hartuta, ahultasunak zerbitzua ukatzea (**DoS**) eta buffer-gainezka egitea ekar lezake, eta, hala, kodea urrunetik (**RCE**) exekutatu ahal izango litzateke RTA urrakorraren EtherNet/IP ezarpen bat exekutatzen duten gailuetan.

EtherNet/IP Forward Open eskaeretan erabilitako bufferraren tamaina mugatuta, fabrikatzaileak RAM erabilera murrizteko egindako saiakerak eragin du akatsa. RAM mugaren bidez, erasotzaile batek bufferra gainditu dezake eta, ondoren, baimendu gabeko aldaketak egin ditzake. Horretarako, erasotzaile batek Forward Open eskaera bat bidali beharko luke, TCP 44818 portuaren bidez bereziki diseinatua. Eskaera hori beharrezkoa da bezeroaren eta azken puntuaren arteko komunikazioa ezartzeko CIP saio beraren bidez. Konexioaren CIP ibilbidea gaizki egiaztatu delako gertatu da akatsa. Hala, erasotzaile batek luzera finkoko bufferretik kanpoko memoriaren helbide batean idazteko aukera izango luke, eta, ondorioz, zerbitzua eten egingo litzateke (DoS), eta,nahiko ahalegin eginez, kodea (RCE) exekutatzeko aukera izango luke.

```
    int i = 0;
    connection_struct.path_size = request->payload[parse_index];

    while (i < connection_struct.path_size) {
        // Stack Overflow: 'path' has size of 32 values, but we can write up to
255 values
        connection_struct.path[i] = ReadWord(request->payload + parse_index);
        parse_index +=2;
        i++;
    }
```

1. irudia. Akatsa ustiatzeko eskatutakoaren antzeko kodea, zaurgarritasuna detektatu zuten segurtasun-ikertzaileek azaldutakoa

Ahultasunak **9.8ko** scorea jaso du **CVSSv3** eskalan oinarrituta; izan ere, urrunetik ustiatzeko aukera ematen du, konplexutasun gutxirekin, ez du erasotzaileak inolako autentifikaziorik eskatzen, eta ez da beharrezkoa erabiltzailearen interakzioa, eta eraso arrakastatsuak eragin osoa izango luke sistemaren konfidentzialtasunean, integritatean eta erabilgarritasunean.

Oraingoz, ez dago jasota akats horri lotutako jarduera maltzurraren gaineko txostenik, ez eta publikoki eskuragarri dagoen exploit edo kontzeptu-probarik dagoenik ere.

499ES EtherNet/IP (ENIP)-ko stack eskualdearen iturburu-kodearen **bertsio** bat, **2.28 baino lehenagokoa** exekutatzen duten gailu guztiei eragiten die; bertsio hori ez dago ukituta, eta Real Time Automation-ek eman zuen **2012an**. Duela urte batzuk RTAk akatsa konpondu bazuen ere, badira oraindik bertsio kaltebera bat ezarria duten gailu asko bere firmwarean. Zaurgarritasuna ekarri zuten ikertzaileen aurkikuntzen arabera, gutxienez 6 hornitzaileko 11 gailuk ENIP bertsio kaltebera erabiltzen dute.

ARINTZEA / KONPONBIDEA

Ahultasuna konpontzeko, 499ES EtherNet/IP (ENIP) stackean ezarritako iturburu-kodearen **azken bertsio egonkorra eguneratu** behar da. Horri dagokionez, Real Time Automation-ek kontrol industrialeko erabiltzaile eta hornitzaileei eskatu die bere ingeniaritza-taldearekin harremanetan jartzeko, 800-249-1612 telefonoaren bidez, ENIP ezarpen ahul bat egiten duten **egiaztatzeko** eta, hala badagokio, **eguneratzeko jarraibideak eskaintzeko**.

Bestalde, Estatu Batuetako Azpiegiturako eta Zibersegurtasuneko Segurtasun Agentziak (CISA) segurtasun-ohar bat egin du, eta, horren bidez, akats horren berri eman du. Horretarako, hainbat arintze-neurri hartu ditu, aurrerantzean deskribatuko direnak:

- Sareko gailu eta/edo sistema guztien esposizioa minimizatzea eta Internetetik eskuragarri ez daudela ziurtatzea.
- Kontrol-sistemak eta urruneko gailuak firewall-aren atzean kokatzea eta erakundearen saretik isolatzea.
- Urruneko sarbidea behar denean, metodo seguruak erabili, hala nola sare pribatu birtualak (VPN), kontuan hartuta VPNek ahultasunak izan ditzaketela eta eskuragarri dagoen azken bertsiora eguneratuta egon behar dutela.

ERREFERENTZIA OSAGARRIAK

- Lingering RTA ENIP stack vulnerability poses risk to ICS devices
- ICS Advisory (ICSA-20-324-03) - Real Time Automation EtherNet/IP
- Secure EtherNet/IP Devices

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?