Treck-en TCP/IP piletako ahultasunak

BCSC_Ahultasunak_Treck_TCP/IP_Pila

TLP:WHITE

www.basquecybersecurity.eus

2020ko Abendua

EDUKI-TAULA

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, 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:

LABURPEN EXEKUTIBOA

Lau ahultasun argitaratu dira, horietako 2 kritikoak, Treck-ek garatutako maila baxuko **TCP/IP** software liburutegi batean. Software hori asmo txarrez erabiliz gero, urruneko erasotzaile bati kodea exekutatzeko edo zerbitzua ukatzeko aukera eman diezaioke (DoS). Treck-en TCP/IP pila mundu osoan dago ezarrita, batez ere, **fabrikazio** sistemetan, **informazioaren teknologietan** eta **osasuna** eta **garraioa** bezalako sektore kritikoetan.

Treck fabrikatzaileak berak gomendatu du pila **6.0.1.68** bertsiora eguneratzea akats horiek konpontzeko, eta, azken partxeak aplikatu ezin badira, hainbat arintze neurri daude, ahultasun horiek aprobetxatzen dituzten erasoen arriskua eta esposizioa murrizteko.

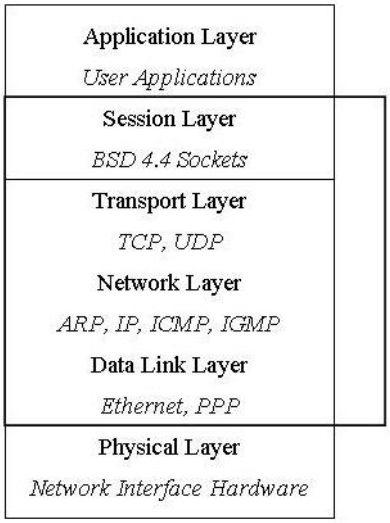
Treck-en TCP/IP pilaren akats berri horiek JSOF zibersegurtasun-konpainiak 19 ahultasun (Ripple20) Treck-en software liburutegi berean jakinarazi eta sei hilabetera argitaratu dira. Horiei esker, IoT gailu espezifikoen gaineko kontrol osoa lor daiteke, erabiltzaile baten interakzioa eskatu gabe.

Gainera, abenduaren hasieran, Forescout enpresako ikertzaileek 33 ahultasun agertu zituzten, AMNESIA:33 kolektiboki deituak, eta kode irekiko TCP/IP protokolo pilei ere eragiten diete. Protokolo horiek ustiatu egin daitezke sistema ahulak kontrolatzeko.

Gailu ahulak errazago atzemateko eta IoT hornitzeko kate konplexua dela eta, Forescout-ek "project-memoria-detector" izeneko detekzio tresna berri bat jarri du martxan, sare objektiboko gailu batek TCP/IP pila ahul bat exekutatzen duen identifikatzeko.

ANALISI TEKNIKOA

Treck-en TCP/IP pila maila baxuko TCP/IP software liburutegia da, eta zehazki diseinatuta dago fabrikazioaren, **ITen, osasunaren eta garraioaren** sektore kritikoetan asko erabiltzen diren **sistema integratuetarako**. Duela gutxi, lau ahultasun berri argitaratu dira, eta horietako bi larritasun kritikotzat jo dira.



1. irudia Treck TCP/IP stack

Errorerik larriena **HTTP** zerbitzariaren **Treck osagaian buferra gainezka egiteko dagoen ahultasuna** da, eta, horri esker, erasotzaileak gailuak berrabiaraz ditzake, bai eta urrunetik kodea exekutatu ere. Ahultasuna CVE-2020-25066 kodearekin eta **9.8ko** scorearekin identifikatu da, **CVSSv3.1** eskalaren arabera.

Bigarren akats larriena **IPv6 osagaian mugetatik kanpo idazteko ahultasuna da**, eta, sare jakin batera sartzearen bidez, zerbitzua ukatzeko baldintza (DoS) sortzeko baimenik ez duen erabiltzaile batek erabil dezake. Ahultasuna CVE-2020-27337 kodearekin eta **CVSSv3.1** eskalaren araberako **9.1** scorearekin identifikatu da.

Gainerako bi ahultasun ez hain larriak **IPv6 osagaian** (CVE-2020-27338, score 5.9 CVSSv3.1) **mugetatik kanpo irakurtzea** ahalbidetzen duten erroreak dira. **Autentifikatu gabeko erasotzaile batek balidatu dezake osagai berean** (CVE-2020-27336, score 3.7 VSSv3.1) zerbitzua ukatzeko eta sarrera desegokia baliozkotzeko. Baliteke hiru byteko mugetatik kanpo irakurtzea, sare jakin baterako sarbidearen bidez.

Hala ere, kontuan hartu behar da ahultasun horiek **gaitasun handia eskatzen dutela ustiatzeko**. Oraingoz, ez da ezagutzen eraso publikorik, exploits erabilgarririk edo horien gaineko kontzeptuen proba espezifikorik.

ARINTZEA / KONPONBIDEA

Treck konpainiak berak gomendatu die erabiltzaileei pila **6.0.1.68 bertsiora edo berriagora** eguneratzeko, ahultasun horiek konpontzeko. Partxeak aplikatu ezin direnean, **HTTP goiburuan eduki negatiboko luzera** duten paketeak iragazteko **firewall arauak ezartzea** gomendatzen da. Partxeak eskuratzeko, mezu elektroniko bat bidali behar da security@treck.com helbidera.

Lehenago aipatu bezala, gailu ahulak errazago atzemateko eta IoT-en hornidura kate konplexuaren aurrean, Forescout-ek "***project-memoria-detector***" izeneko detekzio tresna berri bat merkaturatu du, sare objektiboko gailu batek TCP/IP pila ahul bat exekutatzen duen identifikatzeko.

Gainera, ahultasun horiek ustiatzeko arriskua ahalik eta gehien murrizteko, neurri hauek hartzea gomendatzen da:

- Sareko esposizioa ahalik eta gehien gutxitzea control gailu eta/edo sistema guztiak, eta Internetetik atzitu ezin direla ziurtatzea.
- Kontrol-sistemak eta urruneko gailuak firewall-en atzean kokatzea eta enpresaren saretik isolatzea.
- Urruneko sarbideak behar izanez gero, erabili metodo seguruak, hala nola sare pribatu birtualak (VPN), kontuan hartuta sare horiek ahultasunak izan ditzaketela eta eskuragarri dagoen azken bertsiora eguneratu behar direla.

Horrez gain, kontuan hartu behar da beharrezkoa dela eraginaren azterketa eta arriskuen ebaluazioa egitea defentsa neurri horiek zabaldu aurretik.

Cabe destacar que el US Cybersecurity Infrastructure and Security Agency (CISA) tiene disponible una guía de prácticas recomendadas de seguridad en los sistemas de control. Estas prácticas recomendadas están disponibles para su lectura y descarga, incluyendo mejoras en la ciberseguridad de los **Sistemas de Control Industrial** en base a profundas estrategias de defensa.

Nabarmentzekoa da US Cybersecurity Infrastructure and Security Agency (CISA) erakundeak control sistemetan gomendatutako segurtasun praktiken gida duela. Praktika gomendatu horiek irakurketarako eta deskargarako erabil daitezke, baita **Kontrol Industrialeko Sistemen** zibersegurtasuna hobetzeko ere, defentsa-estrategia sakonetan oinarrituta.

ERREFERENTZIA GEHIGARRIAK

- Treck - VU#114986 and ICS-VU-870237 – Affects versions 6.0.1.67 and earlier
- ICS Advisory (ICSA-20-353-01) - Treck TCP/IP Stack
- Industrial Control Systems - Recommended Practices

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?