AMNESIA:33
Ahultasunak

BCSC-Ahultasunak_

AMNESIA:33

TLP:WHITE

www.basquecybersecurity.eus

2020ko Abendua

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, 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

Forescout enpresako segurtasun-ikertzaileek jakinarazi dute TCP/IP pilek hainbat ahultasun dituztela milioika gailutan, bai sare-ekipoetan, bai gailu medikoetan, bai kontrol industrialeko sistemetan. Sistema horien kontrola hartzeko, erasotzaileek erabil ditzakete.

Modu kolektiboan **"AMNESIA:33"** bezala deituak, aurkitutako akatsak kode irekiko TCP/IP protokoloen (uIP, FNET, picoTCP eta NutNet) lau pilari eragiten dieten **33 ahultasun** multzo bat dira, normalean **IoT gailuetan** erabiltzen direnak.

Memoria modu desegokian kudeatzearen ondorioz, akats horiek behar bezala ustiatzeak memoria hondatzea eragin dezake, eta erasotzaileei gailu horiek arriskuan jartzea, kode maltzurra egitea, zerbitzua ukatzeko erasoak egitea (DoS), informazio sentikorra lapurtzea eta DNSren cache memoria pozoitzea.

Benetako egoera batean, ahultasun horiek ustiatzeak eten egin dezake zentral elektriko baten funtzionamendua edo ke-alarmaren eta tenperatura-kontrolaren sistemak deskonektatzea.

Kalkuluen arabera, **158 fabrikatzaile desberdinen milioi gailu kalteberak dira** AMNESIA:33rekiko, eta enpresa bakar batenak ez diren kode irekiko TCP/IP pila askori eragiten diete.

AZTERKETA TEKNIKOA

TCP/IP pila integratuek funtsezko komunikazio-gaitasuna ematen dute TCP/IP sareetan IoT gailuetan, gailu integratuetan eta *Edge Computing* bezalako teknologietan, hau da, konputazio perimetralean, ezarritako sistema eragile arin askotarako.

TCP/IP pilak IP helbide batera konektatutako gailu guztien osagai larriak dira, oinarrizko sare komunikazioak ahalbidetzen baitituzte.

TCP/IP pila baten segurtasun akatsa oso arriskutsua izan daiteke, osagai horien kodea gailu batera iristen den sare-pakete bakoitza prozesatzeko erabil baitaiteke.

Horrek esan nahi du TCP/IP pila baten zenbait ahultasunek erasotzaile bati gailu bat erabat konprometitzeko aukera eman diezaioketela, baita sare batean aplikazio jakin bat exekutatu gabe dagoenean ere.

1.irudia. "AMNESIA:33" ahultasunak

Ildo horretatik, **AMNESIA:33** IoT, OT eta TI: (**uIP, FNET, picoTCP eta NutNet**) gailuen hornitzaile nagusiek erabiltzen dituzten lau TCP/IP pilen protokoloetan aurkitutako 33 ahultasunen multzoa da.

Ahultasun horiek ustiatuz gero, erasotzaile batek gailu baten kontrola har dezake, eta Internetera konektatutako gailuen sare bateko sarrera-puntu gisa erabil dezake, alboko mugimendurako pibote-puntu gisa, xede sareko iraunkortasungisa edo eraso baten amaierako puntu gisa.

Enpresa-erakundeei dagokienez, horrek esan nahi du nabarmen handitzen dela beren sarea arriskuan jartzeko arriskua, bai eta asmo txarreko aktoreek negozioaren jarraitutasuna ahultzea ere. Erabiltzaile partikularrentzat, horrek esan nahi du haien IoT gailuak eraso-kanpaina handien parte gisa erabil daitezkeela, hala nola botnet-ak, ez dira konturatzen.

Ondoren, AMNESIA:33ren barruan nabarmendu diren 3 ahultasunak aipatzen dira, kritikotzat jo direnak, bakoitzaren deskribapen labur batekin batera:

- **CVE-2020-24336**: NAT64 bidez bidalitako DNS erantzun paketeetan DNS erregistroak aztertzeko kodeak ez du balio erantzun erregistroen luzera eremua, eta, horri esker, erasotzaileek memoria kaltetu dezakete.
- **CVE-2020-24338**: Domeinu-izenak aztertzen dituen funtzioak ez du mugarik egiaztatzen, eta, horri esker, erasotzaileek memoria kaltetu dezakete bereziki diseinatutako DNS paketeekin.
- **CVE-2020-25111**: Bufer-gainezkatze bat gertatzen da pilan. DNSren erantzun-baliabideen erregistro baten izen-eremua prozesatzean gertatzen da hori. Horri esker, erasotzaile batek alboko memoria kaltetu dezake, esleitutako bufer batean byte-kopuru arbitrario bat idatziz.

33 ahultasunei esleitutako CVEen zerrenda osoa, **CVSSv3** eskalan oinarrituta **CISA ICS-CERT** zentroak esleitutako kritikotasunarekin batera, taula honen bidez kontsulta daiteke:

CVE	Kritikotasuna (CVSSv3)
CVE-2020-13984	7.5
CVE-2020-13985	7.5
CVE-2020-13986	7.5
CVE-2020-13987	8.2
CVE-2020-13988	7.5
CVE-2020-17437	8.2
CVE-2020-17438	7.0
CVE-2020-17439	8.1
CVE-2020-17440	7.5
CVE-2020-17441	7.5
CVE-2020-17442	7.5
CVE-2020-17443	8.2
CVE-2020-17444	7.5
CVE-2020-17445	7.5
CVE-2020-17467	8.2
CVE-2020-17468	7.5
CVE-2020-17469	5.9
CVE-2020-17470	4.0
CVE-2020-24334	8.2
CVE-2020-24335	7.5
CVE-2020-24336	**9.8**
CVE-2020-24337	7.5
CVE-2020-24338	**9.8**
CVE-2020-24339	7.5
CVE-2020-24340	8.2
CVE-2020-24341	8.2

CVE-2020-24383	6.5
CVE-2020-25107	7.5
CVE-2020-25108	7.5
CVE-2020-25109	8.2
CVE-2020-25110	8.2
CVE-2020-25111	**9.8**
CVE-2020-25112	8.1

Ahultasun horiek aztertu eta jakinarazteko ardura duten ikertzaileek txosten osoa eta akatsak azaltzen dituen bideoa argitaratu dituzte:

- **Txostena**:
  - https://www.forescout.com/company/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices/
- **Video**:
  - AMNESIA:33 - Forescout

Orain arte ez dakigu ahultasun horien ustiapen aktiboari buruz.

ARINTZEA / KONPONBIDEA

150 fabrikatzaile ukituetako batzuek dagoeneko argitaratu dituzte dagozkien segurtasun-oharrak:

- Devolo
- EMU Electronic AG
- FEIG
- Genetec
- Harting
- Hensoldt
- Microchip
- Nanotec
- NT-Ware
- Tagmaster
- Siemens
- Uniflow
- Yanzi Networks

Gailu kalteberak identifikatzea eta partxeatzea konplexua denez, komeni da irtenbideak hartzea, gailuek ikuspen pikortsua izan dezaten, sareko komunikazioak monitorizatu ahal izateko eta sareko gailu edo segmentu ahulak isolatzeko, ahultasun horiek dakartzaten arriskuak administratzeko.

Gainera, babes-neurri orokorrak hartzea gomendatzen da ahultasun horiek ustiatzeko arriskua minimizatzeko:

- Sareko esposizioa ahalik eta gehiena murrizteko control gailu eta/edo sistema guztiak, eta Internetetik eskuragarri ez daudela ziurtatzeko.
- Kontrol sistemak eta urruneko gailuak firewall-en atzean kokatzea eta enpresa-saretik isolatzea.
- Urruneko sarbidea behar denean, metodo seguruak erabiltzea, hala nola sare pribatu birtualak (VPN), VPNek ahultasunak izan ditzaketela eta eskuragarri dagoen bertsiorik berrienean eguneratu behar direla onartuta.
- Erabili HTTPS gainean DNS egiten duen barneko DNS zerbitzari bat bilaketetarako.

ERREFERENTZIA OSAGARRIAK

- AMNESIA:33. How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices
- ICS Advisory (ICSA-20-343-01) - Multiple Embedded TCP/IP Stacks
- Embedded TCP/IP stacks have memory corruption vulnerabilities - Vulnerability Note VU#815128

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?