



Ahultasunak Cisco-ren telefono egokitzaileetan (SPA112 2)

BCSC-OHARRAK

TLP: CLEAR

www.zibersegurtasun.eus



AURKIBIDEA

BCSCri buruz.....	3
1. Segurtasun oharra.....	4
2. Kaltetutako baliabideak	5
3. Azterketa teknikoa	6
4. Arintzea / Konponbidea	7
5. Erreferentzia Osagarriak.....	8

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, ustekabeen 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

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

BCSCri 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. Segurtasuna, Gobernantza Publiko eta Autogobernua, eta Hezkuntza, bai eta Zientzia, Teknologia eta Berrikuntzako Euskal Sareko eragile ezberdinak ere. Tecnalia, Vicomtech, Ikerlan eta BCAM.



BCSC erreferentziatzko 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 jardura dinamizatzea eta erreferentzia izango den sektore profesional bat sor dadin eragitea. Testuinguru horretan osagarriak diren eragileen arteko lankidetzak proiektuak exekutatzeko 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 analisisian, eta euskal gizartearen beharrak artatzeko beharrezkoak diren prebentzio neurrien diseinuan. Helburu horiek lortzeko xedearekin, zibersegurtasun gertakariak kudeatzera zuzendutako hainbat ekimenetan hartzen du parte:



1. Segurtasun oharra

Ciscok [segurtasun ohar](#) bat argitaratu du, larritasun kritikoko ahultasun bat aztertzen duena. Horren identifikatzailea [CVE-2023-20126](#) da eta [Cisco SPA112 2-Port Phone Adapter](#) produktuari eragiten dio, IP sare baten bidez VoIP zerbitzuen hornitzaile batera telefonoak eta fax makinak konektatzea ahalbidetzen duen telefono analogikoen egokitzaille bat. Ahultasuna baliatuz autentifikatu gabeko urruneko erasotzaile batek kode arbitrarioa exekuta lezake. Horrela, arrakastaz ustiatuz gero, inpaktu handia eragingo litzateke kaltetutako sistemen konfidentzialtasun, integritate eta eskuragarritasunean.

Fabrikatzaileak ez du argitaratu eta ez du argitaratuko azaldutako akatsa konpontzeko eguneraketa edo workaround-ik, produktua bere bizitza zikloaren azkenaldian dagoelako. Ciscok bere bezeroei gomendatzen die [Cisco ATA 190](#) serieko telefono analogikoen egokitzaille batera migratzea.

2. Kaltetutako baliabideak

- Cisco SPA112 2-Port Phone Adapters-en firmware bertsio guztiak.

3. Azterketa teknikoa

Ohar honetan aztertutako ahultasunaren xehetasuna honakoa da:

CVE-2023-20126: Cisco SPA112 telefono egokitzailleek webean oinarritutako administratzaile interfazean duten ahultasuna. Hori baliatuz autentifikatu gabeko urruneko erasotzaile batek kode arbitrarioa exekuta lezake kaltetutako gailu batean. Akatsaren arrazoia da firmwarearen eguneraketa funtzioaren barnean ez egotea autentifikazio prozesurik. Erasotzaile batek ahultasun hau balia lezake kaltetutako gailu bat firmwarearen aldatutako bertsio batera eguneratuz. Ahultasun hau arrakastaz ustiatuz gero, erasotzaileak kaltetutako gailuan kode arbitrarioa exekuta lezake pribilegio guztiekin.

Ahultasunen ebaluazioaren metrika honela osatzen da:

CVSS Base: 9.8

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

- **Eraso bektorea: Sarea**
- **Erasoaren konplexutasuna: Baxua**
- **Behar diren pribilegioak: Batere ez**
- **Erabiltzailearekiko interakzioa: Batere ez**
- **Irismena: Aldaketarik gabe**
- **Konfidentzialtasuna: Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna: Altua**

4. Arintzea / Konponbidea

Ahultasun hauek arintzeko gomendatzen da sistemak eta aplikazioak beti eguneratuta izatea eskuragarri dagoen azken bertsiora, dagozkion eguneraketak argitaratu bezain azkar.

Azaldutako ahultasuna konpontzeko, eta produktua bere bitzta zikloaren amaieran dagoenez gero, Cisco bere bezeroei gomendatzen die [Cisco ATA 190](#) serieko telefono analogikoen egokitzaille batera migratzea.

5. Erreferentzia Osagarriak

- Segurtasun oharra.
- CVE-2023-20126.

 Basque
CyberSecurity
Centre