Basque CyberSecurity Centre

Ahultasunak Cisco produktuetan

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

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:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Laburpen exekutiboa

Ciscok, sareen eta teknologiaren sektorearekin lotutako konpainiak, zazpi segurtasun abisu argitaratu ditu. Horietan, larritasun kritikoko ahultasun bat eta puntuazio altua duten lau akats nabarmentzen dira. Akats horiek honako hauei eragiten diete: Cisco Expressway Series, Cisco TelePresence, Cisco Unified Communications Manager IM and Presence Service, Cisco Adaptative Security Appliance Software and Firepower Threat Defense Software for Firepower 2100 Series Appliances SSL/TLS, Cisco AnyConnect Secure Mobility Client Software Windowserako eta Cisco Secure Client Software Windowserako.

Larritasun kritikoz katalogatutako akatsari dagokionez, identifikatzaile honen pean erregistratu da:

- CVE-2023-20105: urruneko erasotzaile bati Cisco Expressway Series eta Cisco TelePresence VCSn pribilegioak eskalatzeko aukera ematen dion ahultasuna.

Oso larri kalifikatutako ahultasunei dagokienez, identifikatzaile hauekin identifikatu dira:

- CVE-2023-20192: urruneko erasotzaile bati Cisco Expressway Series eta Cisco TelePresence VCSn pribilegioak eskalatzeko aukera ematen dion ahultasuna.
- CVE-2023-20108: zerbitzua ukatzeko baldintza batek (DoS) Cisco Unified Communications Manager IM and Presence Service-n sor dezakeen ahultasuna.
- CVE-2023-20006: zerbitzua ukatzeko baldintza batek (DoS) Cisco Adaptative Security Appliance Software and Firepower Threat Defense Software for Firepower 2100 Series Appliances SSL/TLS eremuan sor dezakeen ahultasuna.
- CVE-2023-20178: urruneko erasotzaile bati Windowserako Cisco AnyConnect Secure Mobility Client Software-n eta Windowserako Cisco Secure Client Software-n pribilegioak eskalatzeko aukera ematen dion ahultasuna.

Fabrikatzaileak dagoeneko argitaratu ditu dagozkion eguneratzeak, eta, hala, akats nabarmenak zuzendu ditu. Beraz, ahultasun horiei eta beste batzuei aurrea hartzeko, komeni da sistemak eta aplikazioak erabilgarri dagoen azken bertsioan eguneratuta izatea, dagozkion adabakiak argitaratu bezain laster.

2. Azterketa teknikoa

Lehenik eta behin, CVE-2023-20105en bidez identifikatutako ahultasuna zehazten da. Ahultasun hori, larritasun kritikoarekin kalifikatua, pasahitza aldatzeko eskaeren kudeaketa desegokiaren ondorioz dago, pasahitza aldatzeko funtzionalitatean. Urruneko erabiltzaile batek bereziki diseinatutako eskaera bat bidal dezake, sisteman edozein erabiltzaileren pasahitzak aldatu eta helburuko erabiltzailea ordeztu.

Lehen deskribatutako ahultasuna ebaluatzeko metrikak honela osatzen dira:

CVSS Oinarria: 9.6

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

- **Eraso bektorea: Sarea**
- **Erasoaren konplexutasuna: Txikia**
- **Eskatutako pribilegioak: Txikia**
- **Erabiltzailearekiko interakzioa: Bat ere ez**
- **Irismena: Aldaketekin**
- **Konfidentzialtasuna:** Bat ere ez
- **Osotasuna: Altua**
- **Erabilgarritasuna: Altua**

Bigarren ahultasuna, zeinaren identifikatzailea CVE-2023-20192 baita, erabiltzaile rolaren baimenak oker esleitzearen ondorioz dagoen akats bat da. Tokiko erabiltzaile batek kode arbitrarioa exekutatu dezake, administratzaile-baimenekin, helmugako sisteman.

Lehen deskribatutako ahultasuna ebaluatzeko metrikak honela osatzen dira:

CVSS Oinarria: 8.4

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

- **Eraso bektorea:** Lokala
- **Erasoaren konplexutasuna: Txikia**
- **Eskatutako pribilegioak: Txikia**
- **Erabiltzailearekiko interakzioa: Bat ere ez**
- **Irismena: Aldaketekin**
- **Konfidentzialtasuna:** Bat ere ez
- **Osotasuna: Altua**
- **Erabilgarritasuna: Altua**

CVE-2023-20108 sisteman erregistratutako errorea erabiltzaileak XCP Autentifikazio Zerbitzuan emandako sarreraren balioztatze eskasaren ondorio da. Urrutiko erasotzaile batek bereziki diseinatutako saio hasierako mezu bat bidal dezake eta zerbitzuaren ukapen eraso bat egin (DoS).

Lehen deskribatutako ahultasuna ebaluatzeko metrikak honela osatzen dira:

CVSS Oinarria: 7.5

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

- **Eraso bektorea: Sarea**
- **Erasoaren konplexutasuna: Txikia**
- **Eskatutako pribilegioak: Bat ere ez**
- **Erabiltzailearekiko interakzioa: Bat ere ez**
- **Irismena:** Aldaketarik ez
- **Konfidentzialtasuna:** Bat ere ez
- **Osotasuna:** Bat ere ez
- **Erabilgarritasuna: Altua**

Laugarren ahultasuna, CVE-2023-20006 sistemarekin identifikatua, SSL/TLS trafikoa prozesatzeko funtzio kriptografikoen barruan inplementazio akats baten ondorioz dago, hardwarera deskargatzen direnean. Urrutiko erasotzaile batek bereziki diseinatutako SSL/TLS trafiko fluxu bat bidali dezake kaltetutako gailu batera, eta zerbitzuaren ukapen eraso bat egin (DoS).

Lehen deskribatutako ahultasuna ebaluatzeko metrikak honela osatzen dira:

CVSS Oinarria: 8.6

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

- **Eraso bektorea: Sarea**
- **Erasoaren konplexutasuna: Txikia**
- **Eskatutako pribilegioak: Bat ere ez**
- **Erabiltzailearekiko interakzioa: Bat ere ez**
- **Irismena: Aldaketekin**
- **Konfidentzialtasuna:** Bat ere ez
- **Osotasuna:** Bat ere ez
- **Erabilgarritasuna: Altua**

Azkenik, CVE-2023-20178ren bidez identifikatutako errorea sistema eguneratzeko prozesuan erabiltzaile rolaren baimenak oker esleitzearen ondorio

da. Tokiko erabiltzaile batek kode arbitrarioa exekutatu dezake, administratzaile-baimenekin, helmugako sisteman.

Lehen deskribatutako ahultasuna ebaluatzeko metrikak honela osatzen dira:

CVSS Oinarria: 7.8

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

- **Eraso bektorea:** Lokala
- **Erasoaren konplexutasuna: Txikia**
- **Eskatutako pribilegioak: Txikia**
- **Erabiltzailearekiko interakzioa: Bat ere ez**
- **Irismena:** Aldaketarik ez
- **Konfidentzialtasuna: Altua**
- **Osotasuna: Altua**
- **Erabilgarritasuna: Altua**

Azkenik, honako hauek dira aurreko ahultasunek kaltetutako produktuak:

- Cisco Expressway Series eta Cisco TelePresence VCS 14.0 bertsioa eta aurrekoak.
- Cisco Unified Communications Manager IM and Presence Service 12.5(1) eta 14SU bertsioak.
- Cisco Adaptative Security Appliance 9.16.4, 9.18.2 eta 9.18.2.5 bertsioak
- Cisco Firepower Threat Defense 7.2.1, 7.2.2 eta 7.2.3 bertsioak
- Cisco AnyConnect Secure Mobility Client Software Windowserako 4.10 bertsioa eta aurrekoak
- Cisco Secure Client Software Windowserako 5.0. bertsioa

3. Arintzea / Konponbidea

Ohiko moduan, ahultasun horiei eta beste batzuei aurrea hartzeko, sistemak eta aplikazioak eskuragarri dagoen azken bertsiora eguneratuta izatea gomendatzen da, eguneratzeak argitaratu bezain laster.

Ciscorekin zuzeneko kontratua duten bezeroek automatikoki jaso beharko dituzte eguneratzeak, duten lizentziaren arabera. Enpresaren produktuak dituzten bezeroak hirugarrenen bidez erosi badira, Ciscoren TACarekin harremanetan jarri beharko dute esteka honen bidez, behar diren zuzenketak egiteko:

- Cisco Worldwide Support Contacts.

Azpimarratzekoa da fabrikatzaileak erabiltzaileei eskatzen diela kaltetutako produktuetan honako bertsio hauek ezartzeko:

- Cisco Expressway Series eta Cisco TelePresence VCS 14.2.1 edo 14.3.0 bertsioa.
- Cisco Unified Communications Manager IM and Presence Service 12.5(1) SU7 edo 14SU3 bertsioak.
- Cisco AnyConnect Secure Mobility Client Software Windowserako 4.10MR7 bertsioa.
- Cisco Secure Client Software Windowserako 5.0MR2 bertsioa.

4. Erreferentzia osagarriak

- Cisco Security Advisories.
- Cisco Expressway Series, Cisco TelePresence.
- Cisco Unified Communications Manager IM and Presence Service.
- Cisco Adaptative Security Appliance Software and Firepower Threat Defense Software for Firepower 2100 Series Appliances SSL/TLS.
- Cisco AnyConnect Secure Mobility Client Software Windowserako.
- Cisco Secure Client Software Windowserako.
- CWE-400: Uncontrolled Resource Consumption.
- CWE-620: Unverified Password Change.
- CWE-20: Improper Input Validation.
- Cisco Worldwide Support Contacts.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA