Basque CyberSecurity Centre

Cisco produktuen ahultasunak

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

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, 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 zerikusia duen konpainiak, hemezortzi segurtasun ohar argitaratu ditu guztira. Horietatik bederatzik bederatzi ahultasun dituzte, eta fabrikatzaileak oso larritzat jotzen ditu. Akats horiek Cisco IOS, Cisco IOS XE, Cisco Access Point eta Cisco DNA-ri eragiten diete.

Larritasun handiz katalogatu diren akatsei dagokienez, identifikatzaile hauen pean erregistratu dira:

- CVE-2023-20027: Cisco IOS XE-n zerbitzua (DoS) ukatzea ekar dezakeen ahultasuna.
- CVE-2023-20065: Tokiko erasotzaile batek bere pribilegioak *root-era* igotzea Cisco IOS XE-n gerta daitekeen ahultasuna.
- CVE-2023-20035: Kode arbitrarioa gauzatzeak Cisco IOS XE SD-WAN-en sor dezakeen ahultasuna.
- CVE-2023-20072: Cisco IOS XE-n zerbitzua (DoS) ukatzea ekar dezakeen ahultasuna.
- CVE-2023-20080: Zerbitzua ukatzeko baldintza batek (DoS) Cisco IOS eta Cisco IOS XE enpresetan sor dezakeen ahultasuna.
- CVE-2023-20067: Cisco IOS XE-n zerbitzua (DoS) ukatzea ekar dezakeen ahultasuna.
- CVE-2023-20055: Ahultasun horrek aukera ematen dio urruneko erasotzaile kautotu bati Cisco DNAn web-ean oinarritutako kudeaketa interfazearen testuinguruan pribilegioak igotzeko.
- CVE-2023-20082: Tokiko erasotzaile bati kode arbitrarioa abiarazte denboran exekutatzeko eta Cisco IOS XE-n konfiantza katea hausteko aukera ematen dion ahultasuna.
- CVE-2023-20112: Ahultasuna, Cisco Access Point-en zerbitzua (DoS) ukatzea ekar dezakeen ustiapena.

Fabrikatzaileak dagoeneko argitaratu ditu dagozkion Segurtasun eguneratzeak, eta, hala, akats nabarmenak zuzendu ditu. Beraz, ahultasun horiei eta beste batzuei aurrea hartzeko, sistemak eta aplikazioak erabilgarri dagoen azken bertsioan eguneratuta edukitzea gomendatzen da.

2. Azterketa teknikoa

Lehenik eta behin, CVE-2023-20027-ren arabera identifikatutako ahultasuna zehazten da. Akats hori badago paketeak gaizki mihiztatzeagatik, *VFR* funtzioa gaituta badago. Urruneko erasotzaile batek pakete zatikatuak bidal ditzake, eta gailua kargatzera behartu; hala, helburu-sisteman zerbitzua ukatzeko baldintza (DoS) da.

Ahultasuna ebaluatzeko metrikak osagai hauek ditu:

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**
- **Beharrezko pribilegioak: Bat ere ez**
- **Erabiltzailearekiko interakzioa: Bat ere ez**
- **Irismena: Aldaketekin**
- **Konfidentzialtasuna:** Bat ere ez
- **Osotasuna:** Bat ere ez
- **Erabilgarritasuna: Altua**

Bigarren ahultasuna, CVE-2023-20065 identifikatzailea duena, akats bat da helmugako sisteman sartzeko behar beste murrizketa ez ezartzeagatik. Tokiko erasotzaile batek pribilegioak eskalatzera irits daiteke, gailu ahulean *root*-rola hartuz.

Ahultasuna ebaluatzeko metrikak osagai hauek ditu:

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**
- **Beharrezko pribilegioak: Txikia**
- **Erabiltzailearekiko interakzioa: Bat ere ez**
- **Irismena:** Aldaketarik ez
- **Konfidentzialtasuna: Altua**
- **Osotasuna: Altua**
- **Erabilgarritasuna: Altua**

Ondoren, CVE-2023-20035-ren arabera identifikatutako ahultasuna sistemaren CLIn sartzeko baliozkotze eskasaren ondorioz sortzen da. Horrek pribilegioak dituen erasotzaile bati kode arbitrarioa exekutatzeko aukera ematen dio, eta horrela, gailu ahula arriskuan jartzen du.

Ahultasuna ebaluatzeko metrikak osagai hauek ditu:

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**
- **Beharrezko pribilegioak: Txikia**
- **Erabiltzailearekiko interakzioa: Bat ere ez**
- **Irismena:** Aldaketarik ez
- **Konfidentzialtasuna: Altua**
- **Osotasuna: Altua**
- **Erabilgarritasuna: Altua**

CVE-2023-20072-n erregistratutako akatsa *tunnel protocol-eko* pakete zatikatuen kudeaketa desegokiak eragin du. Urruneko erasotzaile batek pakete zatikatuak bidal ditzake, eta gailua kargatzera behartu; hala, helburu-sisteman zerbitzua ukatzeko baldintza (DoS) da.

Ahultasuna ebaluatzeko metrikak osagai hauek ditu:

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**
- **Beharrezko pribilegioak: Bat ere ez**
- **Erabiltzailearekiko interakzioa: Bat ere ez**
- **Irismena: Aldaketekin**
- **Konfidentzialtasuna:** Bat ere ez
- **Osotasuna:** Bat ere ez
- **Erabilgarritasuna: Altua**

CVE-2023-20080-an erregistratutako akatsa datuen mugaren sarrera behar bezala baliozkotzen ez delako gertatu da. Urruneko erasotzaile batek manipulatutako *DHCPv6* mezuak bidal ditzake, eta helburu sisteman zerbitzua (DoS) ukatzea eragin dezake.

Ahultasuna ebaluatzeko metrikak osagai hauek ditu:

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**
- **Beharrezko pribilegioak: Bat ere ez**
- **Erabiltzailearekiko interakzioa: Bat ere ez**
- **Irismena: Aldaketekin**
- **Konfidentzialtasuna:** Bat ere ez
- **Osotasuna:** Bat ere ez
- **Erabilgarritasuna: Altua**

Jakinarazitako seigarren ahultasuna, CVE-2023-20067-n erregistratua, helmugako sistemak trafikoaren sarrera behar bezala baliozkotzen ez duelako gertatu da. Urruneko erasotzaile batek bereziki diseinatutako trafikoa bidal dezake, eta helmugako sisteman zerbitzua (DoS) ukatzeko baldintza izan daiteke.

Ahultasuna ebaluatzeko metrikak osagai hauek ditu:

CVSS Oinarria: 7.4

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

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

CVE-2023-20055-ren arabera identifikatutako ahultasuna existitzen da sistema kudeatzeko APIan informazio konfidentziala erakusten delako. Urruneko erasotzaile batek Segurtasun murrizketak saihets ditzake, eta APIra sartu ondoren, pribilegioak mailakatu.

Ahultasuna ebaluatzeko metrikak osagai hauek ditu:

CVSS Oinarria: 8.0

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**
- **Beharrezko pribilegioak: Txikia**
- **Erabiltzailearekiko interakzioa:** Beharrezkoa
- **Irismena:** Aldaketarik ez
- **Konfidentzialtasuna: Altua**
- **Osotasuna: Altua**
- **Erabilgarritasuna: Altua**

CVE-2023-20082-n erregistratutako akatsa, irudiaren sinadura egiaztatzeko erabiltzen den askatzeko gako publikoa berreskuratzean gertatzen diren akatsengatik. Sarbide fisikoa duen erasotzaile batek aldagai espezifikoak alda ditzake serieko interfaze periferikoaren (SPI) flash memorian, eta helburu-sisteman kode arbitrarioa exekutatu.

Ahultasuna ebaluatzeko metrikak osagai hauek ditu:

CVSS Oinarria: 6.1

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

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

Azkenik, CVE-2023-20112 izenarekin identifikatutako akatsa helburu-sisteman parametro batzuk behar bezala balioztatu ez direlako sortu da. Urruneko erasotzaile batek zerbitzua ukatzeko baldintza (DoS) sor dezake.

Ahultasuna ebaluatzeko metrikak osagai hauek ditu:

CVSS Oinarria: 7.4

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

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

Azkenik, ahultasun horiek produktu hauei eragiten diete:

- Cisco IOS XE 17.9.1, 17.9.1a eta 17.9.1.w. bertsioak
- Cisco IOS XE ROM Monitor 17.6.5r. baino lehenagoko bertsioak.
- 1000 Series Integrated Services Routers.
- 4000 Series Integrated Services Routers.
- ASR 1000 Series Aggregation Services Routers.
- Catalyst 8000 Edge Platforms Family.
- Catalyst 8000V Edge Software Routers.
- Catalyst 8200 Series Edge Platforms.
- Catalyst 8300 Series Edge Platforms.
- Catalyst 8500L Series Edge Platforms.

- Catalyst 9300 Series Switches.
- Catalyst 9800 Embedded Wireless Controllers, Catalyst 9300, 9400 eta 9500 Series Switches-entzat.
- Catalyst 9800 Series Wireless Controllers.
- Catalyst 9800-CL Wireless Controllers, Cloud-erako.
- Embedded Wireless Controllers, Catalyst Access Points-en
- Cloud Services Router 1000V Series.
- Cisco DNA Center, konfigurazio lehenetsiarekin.
- Business 150 APs y 151 Mesh Extenders.
- Catalyst 9100 APs.

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.

Cisco-rekin 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.

CVE-2023-20065 erroreari dagokionez, ostatu ingurunea erabiltzen ez duten erabiltzaileei IOX desaktibatzea gomendatzen die Ciscok, *iox ez* den konfigurazio komandoaren bidez.

Nabarmentzekoa da el CVE-2023-20067-ren arabera identifikatutako ahultasunari dagokionez, fabrikatzaileak HTTP bezeroaren profilak sortzeko funtzioa desgaitzea gomendatzen duela, dagozkion segurtasun-eguneratzeak aplikatu ezin badira. Horretarako, erabiltzaileek *Caché HTTP TLV* egiaztatze-aukera kendu beharko dute profil guztietan.

4. Erreferentzia osagarriak

- Cisco IOS XE Software Virtual Fragmentation Reassembly Denial of Service Vulnerability.
- Cisco IOS XE Software IOx Application Hosting Environment Privilege Escalation Vulnerability.
- Cisco IOS XE SD-WAN Software Command Injection Vulnerability.
- Cisco IOS XE Software Fragmented Tunnel Protocol Packet Denial of Service Vulnerability.
- Cisco IOS and IOS XE Software IPv6 DHCP (DHCPv6) Relay and Server Denial of Service Vulnerability.
- Cisco IOS XE Software for Wireless LAN Controllers HTTP Client Profiling Denial of Service Vulnerability.
- Cisco DNA Center Privilege Escalation Vulnerability.
- Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches Secure Boot Bypass Vulnerability.
- Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches Secure Boot Bypass Vulnerability.
- Cisco Access Point Software Association Request Denial of Service Vulnerability.
- Cisco IOS.
- Cisco IOS XE.
- Cisco Access Point.
- Cisco DNA.
- VRF (Virtual Routing and Forwarding).
- CWE-400: Uncontrolled Resource Consumption.
- CWE-284: Improper Access Control.
- CWE-20: Improper Input Validation.
- CWE-94: Improper Control of Generation of Code ('Code Injection').
- First Organization.
- Cisco Worldwide Support Contact.


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA