Basque CyberSecurity Centre

Kalteberatasunak - Cisco BroadWorks CommPilot Application Software eta Cisco Identity Services Engine

BCSC-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

EDUKIAREN TAULA

Erantzukizunetik salbuesteko klausula

Erakundeen eta herritar interesdunen segurtasunaren mesedetan, BCSCk beharrezkotzat jotzen dituen alertak zabaltzeko helburua du honako dokumentu honek. BCSC ez da inola ere erantzule izango emandako informazioa erabiltzeak zuzenean edo zeharka, ustekabean edo ohiz kanpo eragin ditzakeen kalteen gainean, ez eta BCSCren webgunean aipatzen diren teknologiak edo kanpoko informazioa erabiltzeak eragin ditzakeen kalteen gainean ere, baldin eta kanpoko webguneetara, sare sozialetara, software-produktuetara edo alertan edo BCSCren webgunean ager daitekeen beste edozein informaziotara sartzeko estekak baditu. Alertaren edukiak eta mezu elektronikoen bidez eman daitezkeen erantzunak hemen jasotako baldintzen araberako iritzi eta gomendioak dira, eta ezin da jakinarazitako informaziotik ondorio juridiko loteslerik atera.

Salmenta debekatzeko klausula

BCSCri buruz

Zibersegurtasunaren Euskal Zentroa (Basque Cybersecurity Centre, BCSC) Eusko Jaurlaritzak Euskadiko zibersegurtasunaren heldutasun-maila areagotzeko izendatutako erakundea da.

Enpresa Garapenerako Euskal Agentziaren (SPRI) esparruko ekimen transbertsal bat da. Eusko Jaurlaritzako Ekonomiaren Garapen, Jasangarritasun eta Ingurumen Sailaren mendeko sozietate bat da berau. Eusko Jaurlaritzako beste hiru sailekin ere badu harremana: Segurtasun Sailarekin, Gobernantza Publiko eta Autogobernu Sailarekin eta Hezkuntza Sailarekin. Horrez gain, Zientzia, Teknologia eta Berrikuntzaren Euskal Sareko lau eragilerekin ere bai: Tecnalia, Vicomtech, Ikerlan eta BCAM.

BCSC erreferentziako erakundea da Euskadin herritarren, enpresen eta erakunde publikoen zibersegurtasuna eta konfiantza digitala garatzeari dagokionez; batez ere, eskualdeko ekonomian estrategikoak diren sektoreentzat.

BCSCren egitekoa, beraz, euskal gizartean zibersegurtasuna sustatzea eta garatzea da, Euskadiko enpresa-jarduera dinamizatzea, eta erreferente izango den sektore profesional bat sortzea. Testuinguru horretan, berrikuntza teknologikoaren, ikerketaren eta fabrikazio aurreratuko industriara eta beste sektore batzuetara transferentzia teknologikoa egiteko arloetan elkarren osagarri diren eragileen artean lankidetza-proiektuak gauzatzea bultzatzen da.

Era berean, zenbait zerbitzu eskaintzen ditu Gorabeherei Erantzuteko Talde gisa duen rolean (aurrerantzean, CERT, ingelesezko “Computer Emergency Response Team” siglen arabera), eta eginkizun hauek betez aritzen da lanean Euskal Autonomia Erkidegoan: mehatxu berriak detektatzeko eta garaiz ohartarazteko gaitasuna handituz, informazioaren segurtasuneko gorabeherei erantzunez eta horiek analizatuz, eta euskal gizartearen beharrei erantzuteko prebentzio-neurriak diseinatuz. Helburu horiek lortzeko asmoz, zibersegurtasun-gorabeherak kudeatzera bideratutako hainbat ekimenetan hartzen du parte:

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

1. Segurtasun-oharra

Ciscok hainbat segurtasun-abisutan jakinarazi du bere produktuetako biri eragiten dieten kalteberatasun batzuen zuzenketa. Kalteberatasunak larritasun handikoak dira.

Lehenengoek Cisco BroadWorks CommPilot Application Softwareko hutsegiteak zuzentzen dituzte, eta CVE-2022-20951 eta CVE-2022-20958 identifikatzaileak dituzte.

Hurrengoek Cisco Identity Services Engineri eragiten diote, eta CVE-2022-20822 eta CVE-2022-20956 identifikatzaileekin erregistratuta daude. Azkenik, produktu horren barruan, hilabetearen hasieran jakinarazitako kalteberatasun-taldearen informazioari buruzko eguneraketa bat argitaratu da, eta bertan hutsegiteak arintzeko segurtasun-eguneraketak gehitu dira.

2. Eragindako baliabideak

- Cisco BroadWorks CommPilot Application Software
- Cisco ISE

3. Analisi teknikoa

Hona hemen tratatutako kalteberatasunen xehetasunak:

CVE-2022-20958: Cisco BroadWorks CommPilot aplikazio-softwarearen webean oinarritutako administrazio-interfazearen kalteberatasuna: urruneko erasotzaile autentifikatu bati eragindako gailu batean kode arbitrarioa exekutatzeko aukera eman diezaioke, eta erasotzaile batek kalteberatasun hori ustia lezake, HTTP eskaera manipulatu bat bidaliz eragindako gailu baten web-interfazera. Ustiapen arrakastatsuak aukera eman diezaioke erasotzaileari bworks-en erabiltzaile gisa eragindako gailu batean kode arbitrarioa exekutatzeko; horri esker, erasotzaileak fitxategi arbitrarioak irakurri ahal izango lituzke fitxategi-sisteman, edo exekutatzen ari diren prozesuetako batzuk eten.

Kalteberatasunaren metrika hau da:

CVSS Base: 8.3, handia

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

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

CVE-2022-20951: Cisco BroadWorks CommPilot aplikazio-softwarearen webean oinarritutako administrazio-interfazearen kalteberatasuna: autentifikatutako urruneko erasotzaile bati aukera eman diezaioke zerbitzariaren aldetik (SSRF) eskaera faltsifikatzeko eraso bat egiteko eragindako gailu batean. Erasotzaile batek kalteberatasun hori ustia dezake manipulatutako HTTP eskaera bat bidaliz eragindako gailu baten web-interfazera. Ustiapen arrakastatsu batek aukera eman lezake erasotzaileak Cisco BroadWorks zerbitzaritik eta sareko beste gailu batzuetatik informazio konfidentziala eskura dezan.

Kalteberatasunaren metrika hau da:

CVSS Base: 7.7, handia

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

- **Eraso-bektorea: Sarea**
- **Erasoaren konplexutasuna: Txikia**
- **Eskatutako pribilegioak: Txikiak**
- **Erabiltzailearekiko interakzioa**: **Bat ere ez**
- **Irismena: Aldaketekin**

- **Konfidentzialtasuna: Handia**
- **Osotasuna:** Bat ere ez
- **Erabilgarritasuna:** Bat ere ez

CVE-2022-20822: Cisco Identity Services Engine-ren (ISE) webean oinarritutako administrazio-interfazearen kalteberatasuna, autentifikatutako urruneko erasotzaile bati aukera eman diezaiokeena eragindako gailu batean fitxategiak irakurtzeko eta ezabatzeko. Kalteberatasun horren arrazoia da erabiltzaileak emandako sarrera behar bezala ez balidatzea. Erasotzaile batek kalteberatasun hori ustia dezake zenbait karaktere-sekuentzia dituen HTTP eskaera manipulatu bat bidaliz eragindako sistema batera. Ustiapen arrakastatsuak aukera eman diezaioke erasotzaileari gailuan fitxategi espezifikoak irakurtzeko edo ezabatzeko, nahiz eta konfiguratuta duen administrazio-mailak ez liokeen fitxategi horiek atzitzeko aukerarik eman behar.

Kalteberatasunaren metrika hau da:

CVSS Base: 7.1, handia

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N

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

CVE-2022-20956: Cisco Identity Services Engine-ren (ISE) webean oinarritutako administrazio-interfazearen kalteberatasuna; kalteberatasun horrek aukera eman diezaioke autentifikatutako urruneko erasotzaile bati baimena saltatzeko eta sistemaren fitxategietan sartzeko. Kalteberatasun hori eragindako gailu baten webean oinarritutako administrazio-interfazean sarbide-kontrol desegokia egitearen ondorio da. Erasotzaile batek kalteberatasun hori balia dezake manipulatutako HTTP eskaera manipulatu bat bidaliz eragindako gailura. Ustiapen arrakastatsuak aukera eman diezaioke erasotzaileari atzitzerik izan behar ez lukeen fitxategi jakin batzuk zenbakitzeko, deskargatzeko eta ezabatzeko.

Kalteberatasunaren metrika hau da:

CVSS Base: 7.1, handia

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

- **Eraso-bektorea: Sarea**
- **Erasoaren konplexutasuna: Txikia**
- **Eskatutako pribilegioak: Txikiak**

- **Erabiltzailearekiko interakzioa**: **Bat ere ez**
- **Irismena:** Aldaketarik gabe
- **Konfidentzialtasuna: Handia**
- **Osotasuna:** Txikia
- **Erabilgarritasuna:** Bat ere ez

4. Arintzea / Konponbidea

Kalteberatasunak arintzeko, hauxe gomendatzen du BCSCk: dagozkion eguneraketak argitaratu bezain laster, sistemak eta aplikazioak erabilgarri dagoen azken bertsiora eguneratuta edukitzea beti.

Abisuan tratatutako kalteberatasun guztien kasuan –bai Cisco BroadWorks CommPilot Application Software-ri eragiten diotenak, bai Cisco Identity Services Engine-ri eragiten diotenak–, konpainiak kalteberatasunak zuzentzen dituzten software-eguneraketak abiarazi ditu, eta ez da eman hutsegite horiei heltzen dien konponbide alternatiborik.

5. Erreferentzia gehigarriak

- Segurtasun-oharrak
- Cisco BroadWorks CommPilot Application Software
- Cisco Identity Services Engine
- CVE-2022-20951
- CVE-2022-20958
- CVE-2022-20822
- CVE-2022-20956
- Kalteberatasun-taldea


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA