Basque CyberSecurity Centre

Kalteberatasunak - Cisco Identity Services Engine (CVE-2022-20964, CVE-2022-20965, CVE-2022-20966, CVE-2022-20967)

BCSC-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

EDUKIEN TAULA

Erantzukizunetik salbuesteko klausula

Dokumentu hau ematen da BCSCk erakundeen eta herritar interesdunen segurtasunaren alde beharrezkotzat jotzen dituen alertak zabaltzeko. 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 2022ko azaroan argitaratutako segurtasun-abisu baten eguneraketa argitaratu du, Cisco Identity Services Engine (segurtasun-politikak administratzeko plataforma) produktuari eragiten diona. Tratatutako kalteberatasunen artean, larritasun handikoa da CVE-2022-20964 identifikatzailea duena, eta larritasun ertainekoak gainerakoak (CVE-2022-20965,CVE-2022-20966 eta CVE-2022-20967 identifikatzaileak dituztenak).

Hutsegite horiek aukera eman lezakete autentifikatutako urruneko erasotzaile batek sistema eragileko komando arbitrarioak injektatzeko, segurtasun-babesak saihesteko eta guneen arteko komando-sekuentzien erasoak egiteko, eragindako sistemak arriskuan jarriz.

2. Eragindako baliabideak

- Cisco Identity Services Engine

3. Analisi teknikoa

Hona hemen tratatutako kalteberatasunen xehetasunak:

CVE-2022-20964: Cisco ISEren webean oinarritutako administrazio-interfazean komandoak injektatzeko kalteberatasuna, autentifikatutako urruneko erasotzaile bati azpiko sistema eragilean komando arbitrarioak injektatzeko aukera eman diezaiokeena. Horrek eragin dezake erasotzaile horrek, komando-lerrorako sarbidearekin, pribilegioak root-era igotzea eta sistemaren gaineko kontrol osoa lortzea.

Kalteberatasunaren metrika hau da:

CVSS Base: 6.3, handia

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

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

CVE-2022-20966: Cisco ISEren webean oinarritutako administrazio-interfazearen kalteberatasunak aukera eman dezake autentifikatutako urruneko erasotzaile batek komando-sekuentzien erasoak egitea aplikazioaren webean oinarritutako administrazio-interfazearen beste erabiltzaile batzuen aurka. Ustiapen arrakastatsu batek aukera eman dezake erasotzaileak HTML gaiztoa edo aplikazioaren interfazearen barruko komandoen sekuentzia-kodea biltegiratzeko, guneen arteko komando-sekuentzien beste eraso batzuetan erabiltzeko.

Kalteberatasunaren metrika hau da:

CVSS Base: 5.4, ertaina

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

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

CVE-2022-20967: cross-site-scripting kalteberatasuna Cisco ISEren webgunean oinarritutako administrazio-interfazearen kanpoko RADIUS zerbitzariaren funtzioan; aukera eman lezake urruneko erasotzaile autentifikatu batek guneen arteko komando-sekuentzien erasoak egiteko aplikazioaren webgunean oinarritutako administrazio-interfazearen beste erabiltzaile batzuen aurka. Ustiapen arrakastatsu batek aukera eman dezake erasotzaileak HTML gaiztoa edo aplikazioaren interfazearen barruko komandoen sekuentzia-kodea biltegiratzeko, guneen arteko komando-sekuentzien beste eraso batzuetan erabiltzeko.

Kalteberatasunaren metrika hau da:

CVSS Base: 4.8, ertaina

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

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

CVE-2022-20965: Cisco ISEren webean oinarritutako administrazio-interfazeko bypass kalteberatasuna; aukera eman diezaioke autentifikatutako urruneko erasotzaile bati webean oinarritutako administrazio-interfazearen barruko segurtasun-murrizketak saihesteko. Ustiapen arrakastatsu batek aukera eman diezaioke erasotzaileari webean oinarritutako administrazio-interfazearen barruan ekintza pribilegiatuak egiteko, bestela murriztuta egon beharko luketenak.

Kalteberatasunaren metrika hau da:

CVSS Base: 4.3, ertaina

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

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

Ciscok azpimarratzen du konpainiak software-eguneraketak abiaraztea aurreikusten duela abisu honetan deskribatutako kalteberatasunei aurre egiteko, eta, oraingoz, ez dagoela hutsegite horiei erantzuteko ordezko konponbiderik.

Horrez gain, bezeroei gomendatzen zaie baliozko lizentzia duen softwarea soilik deskargatzea, Ciscotik zuzenean edo Ciscoren banatzaile edo bazkide baimendu baten bidez lortua.

5. Erreferentzia gehigarriak

- Cisco-ren segurtasun-abisua
- Cisco Identity Services Engine
- CVE-2022-20964
- CVE-2022-20965
- CVE-2022-20966
- CVE-2022-20967


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA