Basque CyberSecurity Centre

Ahultasuna FortiOS-en (CVE-2022-42475)

BCSC-OHARRAK

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. Segurtasuna, Gobernantza Publiko eta Autogobernua, eta Hezkuntza, bai eta Zientzia, Teknologia eta Berrikuntzako Euskal Sareko eragile ezberdinak 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, 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 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. Segurtasun oharra

Fortinet-ek larritasun kritikoko eta 9.3 CVSS-ko ahultasun bat konpontzen duen segurtasun eguneraketa bat argitaratu du. Ahultasuna FortiOS-en heap-ean oinarritzen den bufferraren gainezkatze erakoa da, eta bere identifikatzailea CVE-2022-42475 da.

Bestalde, konpainiak ezagutzera emandako segurtasun oharrean adierazten den moduan, akatsa **baliatua** izaten ari da.

2. Kaltetutako baliabideak

- FortiOS-en honako bertsioak: 7.2.2, 7.2.1, 7.2.0, 7.0.8, 7.0.7, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 6.4.9, 6.4.8, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.10, 6.4.1, 6.4.0, 6.2.9, 6.2.8, 6.2.7, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.11, 6.2.10, 6.2.1, 6.2.0

3. Azterketa teknikoa

CVE-2022-42475 identifikatzailearekin izendatutako ahultasuna FortiOS SSL-VPN-n oinarritzen den bufferraren gainezkatze erakoa da. Horren bitartez, autentifikatu gabeko urruneko erasotzaile batek kodea edo komando arbitrarioak exekuta ditzake bereziki diseinatutako eskaeren bidez, eta akats hori balia dezake eguneratuta ez dagoen sistema baten kontrola hartzeko.

Ahultasunaren metrika honakoa da:

CVSS Oinarrizkoa: 9.3, kritikoa

CWE-122: Heap-ean oinarritutako bufferraren gainezkatzea

4. Arintzea / Konponbidea

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

Horregatik, akats honen kritikotasuna dela eta, Fortinet-ek bere bezeroei gomendatzen die konpainiak eskainitako eguneraketa ezartzea eta konpromisozko ondoko adierazleak egiaztatzea:

- Erregistro sarrera (log) anitzak honakoarekin:

  Logdesc="Application crashed" and msg="[...] application:sslvpnd,[...], Signal 11 received, Backtrace: [...]“

- Fitxategien sisteman ondorengo artefaktuak egotea:

  /data/lib/libips.bak
  /data/lib/libgif.so
  /data/lib/libiptcp.so
  /data/lib/libipudp.so
  /data/lib/libjepg.so
  /var/.sslvpnconfigbk
  /data/etc/wxd.conf
  /flash

- IP helbide susmagarrietarako konexioak FortiGate-tik:

  188.34.130.40:444

  103.131.189.143:30080,30081,30443,20443

  192.36.119.61:8443,444

  172.247.168.153:8033

5. Erreferentzia Osagarriak

- CVE-2022-42475
- Fortinet-en segurtasun oharra
- FortiOS
- CWE-122


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA