Basque CyberSecurity Centre

Ahultasunak Fortinet produktuetan

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

BCSCri 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

Fortinetek hainbat segurtasun ohar argitaratu ditu: FG-IR-23-001, FG-IR-22-281, FG-IR-22-309, FG-IR-22-401, FG-IR-23-050 eta FG-IR-22-254. Horien artetik lehenengoan FortiOS eta FortiProxy-k duten ahultasun kritiko bat aztertzen da, CVE-2023-25610 identifikatzailea duena. Gainerakoetan larritasun altuko akatsak zuzentzen dira, FortiNAC, ForiSOAR eta FortiWeb produktuei eta baita FortiOS eta FortiProxy-ri ere eragiten dietenak. Horien identifikatzaileak honakoak dira: CVE-2022-39953, CVE-2022-42476, CVE-2023-25605, CVE-2022-39951 eta CVE-2022-40676. Ahultasun horiek baliatuz zerbitzuaren ukapen egoera, pribilegioen eskalatzea, baimendu gabeko kode edo komandoen exekuzioa eta sarbidearen kontrol desegokia sor litezke, eta horiek guztiek sistemen konfidentzialtasunari eragingo liokete.

Fabrikatzaileak dagoeneko argitaratu ditu dagozkion eguneraketak eta workaround-ak, eta horien bitartez zuzendu egin dira aipatutako akatsak.

2. Kaltetutako baliabideak

- FortiOS, 7.2.0 bertsiotik 7.2.3 bertsiora bitartekoak.
- FortiOS, 7.0.0 bertsiotik 7.0.9 bertsiora bitartekoak.
- FortiOS, 6.4.0 bertsiotik 6.4.11 bertsiora bitartekoak.
- FortiOS, 6.2.0 bertsiotik 6.2.12 bertsiora bitartekoak.
- FortiOS 6.0 bertsio guztiak.
- FortiProxy, 7.2.0 bertsiotik 7.2.2 bertsiora bitartekoak.
- FortiProxy, 7.0.0 bertsiotik 7.0.8 bertsiora bitartekoak.
- FortiProxy, 2.0.0 bertsiotik 2.0.11 bertsiora bitartekoak.
- FortiProxy 1.2 bertsio guztiak.
- FortiProxy 1.1 bertsio guztiak.
- FortiNAC 9.4.0 bertsioa.
- FortiNAC, 9.2.0 bertsiotik 9.2.5 bertsiora bitartekoak.
- FortiNAC, 9.1.0 bertsiotik 9.1.8 bertsiora bitartekoak.
- FortiNAC, 8.8, 8.7, 8.6, 8.5, 8.3 bertsio guztiak.
- FortiNAC, 9.4.0 bertsiotik 9.4.1 bertsiora bitartekoak.
- FortiNAC, 9.2.0 bertsiotik 9.2.6 bertsiora bitartekoak.
- FortiNAC, 9.1.0 bertsiotik 9.1.8 bertsiora bitartekoak.
- FortiNAC, 8.8, 8.7, 8.6, 8.5, 8.3 bertsio guztiak.
- FortiOS, 7.2.0 bertsiotik 7.2.3 bertsiora bitartekoak.
- FortiOS, 7.0.0 bertsiotik 7.0.8 bertsiora bitartekoak.
- FortiOS, 6.4.0 bertsiotik 6.4.11 bertsiora bitartekoak.
- FortiOS, 6.2.0 bertsiotik 6.2.12 bertsiora bitartekoak.
- FortiProxy, 7.2.0 bertsiotik 7.2.1 bertsiora bitartekoak.
- FortiProxy, 7.0.0 bertsiotik 7.0.7 bertsiora bitartekoak.
- FortiProxy, 2.0.0 bertsiotik 2.0.11 bertsiora bitartekoak.
- FortiProxy, 1.2.0 bertsiotik 1.2.13 bertsiora bitartekoak.
- FortiProxy, 1.1.0 bertsiotik 1.1.6 bertsiora bitartekoak.
- FortiSOAR, 7.3.0 bertsiotik 7.3.1 bertsiora bitartekoak.
- FortiWeb, 7.0.0 bertsiotik 7.0.2 bertsiora bitartekoak.
- FortiWeb, 6.3.6 bertsiotik 6.3.20 bertsiora bitartekoak.

- FortiWeb 6.4 bertsio guztiak.

3. Azterketa teknikoa

Eguneraketa honetan aztertutako ahultasunen xehetasunak honakoak dira:

CVE-2023-25610: FortiOS eta FortiProxy-ren interfaze administratzailean dagoen bufferraren gainezkatze erako ahultasuna. Hori baliatuz autentifikatu gabeko urruneko erasotzaile batek kode arbitrarioa exekuta lezake gailuan edota zerbitzuaren ukapen egoera (DoS) eragin lezake GUIan, bereziki diseinatutako eskaeren bidez. Ez da ezagutzen ahultasun hau baliatua izan den kasurik.

Ahultasunaren ebaluazioaren metrika honela osatzen da:

CVSS Oinarrizkoa: 9.3

CVE-2022-39953: FortiNAC-ek duen pribilegioen eskalatze erako ahultasuna. Hori baliatuz pribilegio baxuak lituzkeen baina shell-era sarbidea lukeen erabiltzaile lokal batek komando arbitrarioak exekuta litzake root modura.

Ahultasunaren ebaluazioaren metrika honela osatzen da:

CVSS Oinarrizkoa: 7.8

CWE 269: Improper Privilege Management

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

- **Eraso bektorea:** Lokala
- **Erasoaren konplexutasuna: Baxua**
- **Behar diren pribilegioak: Baxuak**
- **Erabiltzailearekiko interakzioa: Batere ez**
- **Irismena:** Aldaketarik gabe
- **Konfidentzialtasuna: Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna: Altua**

CVE-2022-42476: FortiOS-ek eta FortiProxy-k duten bide erlatiboaren ibilbide erako ahultasuna. Hori baliatuz VDOMen administratzaile pribilegiatuek beren pribilegioak eskalatu ditzakete superadministratzaile mailara, diseinatutako CLI eskaeren bidez.

Ahultasunaren ebaluazioaren metrika honela osatzen da:

CVSS Oinarrizkoa: 7.8

CWE 23: Relative Path Traversal

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

- **Eraso bektorea:** Lokala
- **Erasoaren konplexutasuna: Baxua**
- **Behar diren pribilegioak:** Altuak
- **Erabiltzailearekiko interakzioa: Batere ez**

- **Irismena: Aldaketekin**
- **Konfidentzialtasuna: Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna: Altua**

CVE-2023-25605: FortiSOAR-ek playbook osagaian duen sarbidearen kontrol oker erako ahultasuna. Hori baliatuz interfaze administratzailean autentifikatuta dagoen erasotzaile batek baimendu gabeko ekintzak egin litzake diseinatutako HTTP eskaeren bidez.

Ahultasunaren ebaluazioaren metrika honela osatzen da:

CVSS Oinarrizkoa: 7.5

CWE 284: Improper Access Control

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

- **Eraso bektorea: Sarea**
- **Erasoaren konplexutasuna: Baxua**
- **Behar diren pribilegioak: Batere ez**
- **Erabiltzailearekiko interakzioa: Batere ez**
- **Irismena:** Aldaketarik gabe
- **Konfidentzialtasuna: Altua**
- **Integritatea:** Batere ez
- **Eskuragarritasuna:** Batere ez

CVE-2022-39951: FortiWeb-ek duen sistema eragileko komandoen injekzio erako ahultasuna. Hori baliatuz autentifikatutako erabiltzaileek baimendu gabeko kodea edo komandoak exekuta litzakete bereziki diseinatutako HTTP eskaeren bidez.

Ahultasunaren ebaluazioaren metrika honela osatzen da:

CVSS Oinarrizkoa: 7.2

CWE 78: Improper Neutralization of Special Elements used in an OS Command (OS Command Injection)

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

- **Eraso bektorea: Sarea**
- **Erasoaren konplexutasuna: Baxua**
- **Behar diren pribilegioak:** Altuak
- **Erabiltzailearekiko interakzioa: Batere ez**
- **Irismena:** Aldaketarik gabe
- **Konfidentzialtasuna: Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna: Altua**

CVE-2022-40676: FortiNAC-ek duen Cross site scripting XSS erako ahultasuna. Hori baliatuz autentifikatutako erabiltzaile batek XSS eraso bat egin lezake diseinatutako HTTP eskaeren bidez.

Ahultasunaren ebaluazioaren metrika honela osatzen da:

CVSS Oinarrizkoa: 7.1

CWE 79: Improper Neutralization of Input During Web Page Generation (Cross-site Scripting)

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

- **Eraso bektorea: Sarea**
- **Erasoaren konplexutasuna:** Altua
- **Behar diren pribilegioak: Batere ez**
- **Erabiltzailearekiko interakzioa:** Beharrezkoa
- **Irismena:** Aldaketarik gabe
- **Konfidentzialtasuna: Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna: Altua**

4. Arintzea / Konponbidea

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

FG-IR-23-001 oharrean aztertutako ahultasun kritikoaren kasuan, Fortinetek honakoa gomendatzen du:

- FortiOS 7.4.0 edo goragoko bertsio batera eguneratzea.
- FortiOS 7.2.4 edo goragoko bertsio batera eguneratzea.
- FortiOS 7.0.10 edo goragoko bertsio batera eguneratzea.
- FortiOS 6.4.12 edo goragoko bertsio batera eguneratzea.
- FortiOS 6.2.13 edo goragoko bertsio batera eguneratzea.
- FortiProxy 7.2.3 edo goragoko bertsio batera eguneratzea.
- FortiProxy 7.0.9 edo goragoko bertsio batera eguneratzea.
- FortiProxy 2.0.12 edo goragoko bertsio batera eguneratzea.
- FortiOS-6K7K 7.0.10 edo goragoko bertsio batera eguneratzea.
- FortiOS-6K7K 6.4.12 edo goragoko bertsio batera eguneratzea.
- FortiOS-6K7K 6.2.13 edo goragoko bertsio batera eguneratzea.

FortiOS-en kasuan beste konponbide bat ere eskaintzen da, oharrean bertan eskuragarri dagoena.

FG-IR-22-281 oharrean aztertutako ahultasunaren kasuan, Fortinetek honakoa gomendatzen du:

- FortiNAC 9.4.1 edo goragoko bertsio batera eguneratzea.
- FortiNAC 9.2.6 edo goragoko bertsio batera eguneratzea.
- FortiNAC 9.1.9 edo goragoko bertsio batera eguneratzea.
- FortiNAC 7.2.0 edo goragoko bertsio batera eguneratzea.

FG-IR-22-309 oharraren kasuan Fortinetek honakoa gomendatzen du:

- FortiNAC 9.4.2 edo goragoko bertsio batera eguneratzea.
- FortiNAC 9.2.7 edo goragoko bertsio batera eguneratzea.
- FortiNAC 9.1.9 edo goragoko bertsio batera eguneratzea.
- FortiNAC 7.2.0 edo goragoko bertsio batera eguneratzea.

FG-IR-22-401 oharrari dagokionez Fortinetek honakoa gomendatzen du:

- FortiProxy 7.2.2 edo goragoko bertsio batera eguneratzea.
- FortiProxy 7.0.8 edo goragoko bertsio batera eguneratzea.
- FortiOS 7.2.4 edo goragoko bertsio batera eguneratzea.
- FortiOS 7.0.9 edo goragoko bertsio batera eguneratzea.
- FortiOS 6.4.12 edo goragoko bertsio batera eguneratzea.
- FortiOS 6.2.13 edo goragoko bertsio batera eguneratzea.

FG-IR-23-050 oharraren kasuan Fortinetek honakoa gomendatzen du:

- FortiSOAR 7.3.2 edo goragoko bertsio batera eguneratzea.

Azkenik, FG-IR-22-254 oharrari dagokionez Fortinetek honakoa gomendatzen du:

- FortiWeb 7.2.0 edo goragoko bertsio batera eguneratzea.
- FortiWeb 7.0.3 edo goragoko bertsio batera eguneratzea.
- FortiWeb 6.3.21 edo goragoko bertsio batera eguneratzea.

5. Erreferentzia Osagarriak

- FG-IR-23-001.
- FG-IR-22-281.
- FG-IR-22-309.
- FG-IR-22-401.
- FG-IR-23-050.
- FG-IR-22-254.
- CVE-2023-25610.
- CVE-2022-39953.
- CVE-2022-42476.
- CVE-2023-25605.
- CVE-2022-39951.
- CVE-2022-40676.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA