Basque CyberSecurity Centre

BIG-IP eta BIG-IQeko kalteberatasunak (CVE-2022-41622, CVE-2022-41800)

BCSC-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

GRUPO spri TALDEA

EDUKIEN TAULA

Erantzukizunetik salbuesteko klausula

BCSCren aburuz erakundeen eta herritar interesdunen segurtasunerako beharrezkoak diren alertak zabaltzea du helburu 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 terminoekin bat datozen iritziak eta gomendioak dira, eta emandako informaziotik ezin da 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 Intzidenteei 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

F5 segurtasun-hornitzaileak berrikuspenak argitaratu ditu bi kalteberatasunetarako :CVE-2022-41622 eta CVE-2022-41800, BIG-IP eta BIG-IQ sareko gailuei eragiten dietenak, eta kodearen urruneko exekuzioa (RCE) eta gailuaren murrizketen bypassa eragin dezaketenak, hurrenez hurren. Konpainiak hutsegite larrienari esleitu dio -CVE-2022-41622 identifikatzailearekin- 8.8ko CVSS puntuazioa, larritasun handiarekin. Bigarrenak, CVE-2022-41800 identifikatzailea duenak, 8.7ko CVSS puntuazioa du, larritasun handikoa baita ere.

2. Eragindako baliabideak

- BIG IPko modulu guztiak, 17.0.0 bertsioa, 16.1.0tik 16.1.3ra bitarteko bertsioak, 15.1.0tik 15.1.8ra bitartekoak, 14.1.0tik 14.1.5era bitartekoak eta 13.1.0tik 13.1.5era bitartekoak.
- BIG-IQ Centralized Management, 8.0.0tik 8.2.0ra bitartekoak, 7.1.0 bertsioa (CVE-2022-41622 identifikatzailea duen kalteberatasunerako soilik)

3. Analisi teknikoa

CVE-2022-41622 gisa identifikatutako kalteberatasuna bat dator BIG-IP eta BIG-IQ kodearen urruneko exekuzio-hutsegitearekin, guneen arteko eskaerak faltsifikatzeko erasoekiko kalteberak direnak. Horrela, erasotzaile batek engaina ditzake erabiltzaileak, gutxienez baliabide-administratzailearen rol-pribilegioak dituztenak, eta iControl SOAP-en oinarrizko autentifikazioaren bidez autentifikatzen direnak ekintza kritikoak egiteko. Erasotzaile batek kalteberatasun hori kontrol-planoaren bidez soilik balia dezake, ez datuen planoaren bidez. Ustiatzen bada, kalteberatasunak sistema osoa arriskuan jar dezake.

Kalteberatasuna ezkutuan dago, xehetasunak argitaratu zain. Hauek dira ezagutzen diren datuak:

CVSS Base: 8.8, handia

CWE: 352 Cross-Site Request Forgery (CSRF)

CVE-2022-41800ri dagokionez, Administratzailearen funtzioari esleitutako autentifikatutako erabiltzaile batek Gailu moduaren murrizketak saihets ditzakeenean sortzen den kalteberatasuna da, adierazi gabeko iControl-en azken puntu bat erabiliz; horrela, Gailu moduan, autentifikatutako erabiltzaile batek administratzailearen rolari esleitutako erabiltzaile-kredentzial baliodunak saihets ditzake gailu moduaren murrizketak saihesteko. Gailu modua lizentzia espezifiko baten bidez aplikatzen da, edo banakako klusterreko (vCMP) prozesu anitzeko gonbidatuen instantzietarako gaitu edo desgaitu daiteke. **Ustiapen arrakastatsu batek aukera eman diezaioke erasotzaileari segurtasun-muga bat gurutzatzeko**

Kalteberatasuna ezkutuan dago, xehetasunak argitaratu zain. Hauek dira ezagutzen diren datuak:

CVSS Base: 8.7, handia

CWE: 77 Improper Neutralization of Special Elements used in a Command ('Command Injection')

4. Arintzea / Konponbidea

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

CVE-2022-41622 hutsegitea arintzeko, web-nabigatzaile bakar eta isolatu bat erabil daiteke BIG-IP edo BIG-IQ sistema administratzean, kontuan hartuz eraso bat ezin dela prebenitu iControl SOAPen autentifikatu bada oinarrizko autentifikazioa duen web-nabigatzailean. Autentifikazio-mekanismo hori ez da oso arrunta, eta saio-hasierako orriaren erabilerarekiko desberdina da konfigurazioaren erabilgarritasunerako. **F5-etik gomendatzen da web-nabigatzailean oinarrizko autentifikazioarekin ez autentifikatzea. Oinarrizko autentifikaziorako autentifikazio-leiho bat agertzen bada web-nabigatzailean, ez dira kredentzialak eman behar.**

Gomendatzen da jardunbiderik onenak jarraitzea administrazio-interfazerako sarbidea eta BIG-IP eta BIG-IQ sistemen beraren IP helbideak ziurtatzeko; horrek eraso-azalera minimizatzen lagunduko du. Informazio xehatua eskainitako segurtasun-abisuan dago.

CVE-2022-41800 kalteberatasunari dagokionez, F5etik ezartzen da bertsio finko bat instalatu arte aldi baterako arintze batzuk kontsulta daitezkeela segurtasun-abisuan. Arintze horiek iControl RESTerako sarbidea murrizten dute soilik sare edo gailu fidagarrietara, eta horrek eraso-azalera mugatzen du. Erasotzaileak pribilegio asko dituen administrazio-kontu baterako baliozko kredentzialak izan behar ditu; beraz, sarbidea murrizteak tarte fidagarriaren barruan konprometituta dagoen beste gailu baten barne-mugimendu gaizto baten edo alboko barne-mugimendu baten arriskupean utz dezake oraindik gailua.

5. Erreferentzia gehigarriak

- CVE-2022-41622 kalteberatasunaren segurtasun-abisua
- CVE-2022-41800 kalteberatasunaren segurtasun-abisua
- CVE-2022-41622
- CVE-2022-41800
- iControl SOAP
- iControl REST

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA