Basque CyberSecurity Centre

VMware Cloud Foundation kalteberatasunak (CVE-2021-39144, CVE-2022-31678)

BCSC-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

EDUKIAREN TAULA

Erantzukizunetik salbuesteko klausula

Dokumentu hau ematen da BCSCk erakundeen eta herritar interesdunen segurtasunaren alde beharrezkotzat jotzen dituen alertak zabaltzeko. BCSC ezin da inola ere jo zuzenean edo zeharka, ustekabean edo ohiz kanpo jakinarazitako informazioa erabiltzeak eragin ditzakeen kalteen erantzuletzat, ez eta BCSCren webgunetik nahiz kanpoko informaziotik (kanpoko web-orrietarako, sare sozialetarako, software-produktuetarako edo BCSCren alertaren edo webgunearen bidez ager daitekeen beste edozein informaziotarako esteken bidez) aipatzen diren teknologien erantzuletzat ere. Nolanahi ere, alertaren edukiak eta mezu elektronikoen bidez eman daitezkeen erantzunak hemen jasotako terminoen araberako iritziak eta gomendioak dira, eta ezingo da ondorio juridiko loteslerik sortu jakinarazitako informaziotik.

Saltzeko debekuaren klausula

BCSCri buruz

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

Zeharkako ekimena da, Eusko Jaurlaritzako Ekonomiaren Garapen, Jasangarritasun eta Ingurumen Sailaren mendekoa den Enpresen Garapenerako Euskal Agentziaren (SPRI) barruan dagoena. Era berean, Eusko Jaurlaritzako beste hiru sail ere sartzen dira ekimenean –Segurtasuna, Gobernantza Publikoa eta Autogobernua eta Hezkuntza Saila–, eta Zientzia, Teknologia eta Berrikuntzaren Euskal Sareko lau eragile: Tecnalia, Vicomtech, Ikerlan eta BCAM.

BCSC erreferentzia-erakundea da Euskadiko herritarren, enpresen eta erakunde publikoen zibersegurtasuna eta konfiantza digitala garatzeko, bereziki eskualdeko ekonomiaren sektore estrategikoentzat.

BCSCren egitekoa da, beraz, euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa-jarduera dinamizatzea eta erreferentea izango den sektore profesional bat sortzea ahalbidetzea. Testuinguru horretan, eragile osagarrien arteko lankidetza-proiektuak gauzatzea bultzatzen da, berrikuntza teknologikoaren, ikerketaren eta fabrikazio aurreratuko industriarako eta beste sektore batzuetarako transferentzia teknologikoaren eremuetan.

Era berean, hainbat zerbitzu eskaintzen ditu Gorabeherei erantzuteko lantalde gisa (aurrerantzean CERT: “Computer Emergency Response Team” ingelesezko siglak), eta Euskal Autonomia Erkidegoaren esparruan lan egiten du mehatxu berriak detektatzeko eta garaiz ohartarazteko gaitasuna handitzen, informazioaren segurtasun-gorabeheren erantzuna eta analisia egiten, eta euskal gizartearen beharrei erantzuteko prebentzio-neurriak diseinatzen. Helburu horiek lortzeko, zibersegurtasun-gorabeherak kudeatzera bideratutako hainbat ekimenen parte da:

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

1. Segurtasun-abisua

VMware-k bi kalteberatasunetarako (CVE-2021-39144, CVE-2022-31678 identifikatzaileak) eguneraketa argitaratu du bere segurtasun-abisuen bidez. Lehena kritikoa da (CVSS: 9.8).

2. Eragindako baliabideak

- VMware Cloud Foundation (Cloud Foundation)
- VMware Cloud Foundation (NSX-V)

3. Analisi teknikoa

CVE-2021-39144 gisa identifikatutako kalteberatasuna bat dator XStream kode irekiko liburutegiaren bidez urrunetik kodea exekutatzeko hutsegite batekin; horrek esan nahi du autentifikatu gabeko azken puntu batek XStream baliatzen duela VMware Cloud Foundation-en (NSX-V) sarrera serializatzeko. Beraz, eragile gaizto batek kodearen urruneko exekuzioa lor dezake gailuko root testuinguruan.

Kalteberatasuna ebaluatzeko metrika hau da:

CVSS Base: 9.8, kritikoa

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

- **Eraso-bektorea**: **Sarea**
- **Erasoaren konplexutasuna**: Handia
- **Eskatutako pribilegioak:** Txikiak
- **Erabiltzailearekiko interakzioa**: **Bat ere ez**
- **Irismena: Aldaketekin**
- **Konfidentzialtasuna: Handia**
- **Integritatea: Handia**
- **Eskuragarritasuna: Handia**

CVE-2022-31678ri dagokionez, XML (XXE) kanpo-entitateko kalteberatasun bat dauka; hau da, autentifikatu gabeko erabiltzaile batek arazo hori ustiatu eta zerbitzua ukatzeko edo informazioa zabaltzeko baldintza eragin dezake. VMware-n hutsegite horren larritasuna ebaluatu da, eta **kritikotasun moderatu**kotzat jo da (oinarrizko puntuazioa: CVSSv3 5.3).

4. Arintzea / Konponbidea

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

Horregatik, VMware-k bi hutsegiteak konpontzen dituzten segurtasun-adabakiak jarri ditu bere segurtasun-abisuan.

5. Erreferentzia gehigarriak

- Segurtasun-abisua
- CVE-2021-39144
- CVE-2022-31678

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA