Basque CyberSecurity Centre

Ahultasunak VMware 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

VMware-k bi segurtasun ohar argitaratu ditu, VMSA-2023-0004 eta VMSA-2023-0005, larritasun kritikoko ahultasun bat eta larritasun altuko beste bat aztertzen dituztenak, hurrenez hurren. Larritasun kritikoaren identifikatzailea CVE-2023-20858 da eta altuarena CVE-2023-20855.

Alde batetik, CVE-2023-20858 akats kritikoa baliatuz asmo gaiztoko eragile batek kodea injekta lezake Carbon Black App Control tresnaren administrazio kontsolaren bidez. Beste alde batetik, CVE-2023-20855 akatsa baliatuz informazio sentikorrera sarbidea eskura liteke edo pribilegioen eskalatzea lortu. Bi kasuetan, ahultasun horiek baliatuz gero kaltetutako sistemen konfidentzialtasun, integritate eta eskuragarritasunean inpaktu handia eragingo litzateke.

2. Kaltetutako baliabideak

- VMware vRealize Orchestrator 8.x bertsioa.
- VMware vRealize Automation 8.x bertsioa.
- VMware Cloud Foundation (Cloud Foundation) 4.x bertsioa.
- VMware Carbon Black App Control (App Control) 8.7.x, 8.8.x eta 8.9.x bertsioak.

3. Azterketa teknikoa

Eguneraketa honetan aztertutako ahultasunen xehetasunak honakoak dira:

CVE-2023-20858: kodearen injekzio erako ahultasuna. Horren bitartez, App Control administrazio kontsolara sarbide pribilegiatua lukeen asmo gaiztoko eragile batek bereziki diseinatutako sarrera bat erabil lezake, azpiko zerbitzariaren sistema eragilerako sarbidea ahalbidetuko lukeena.

Ahultasunaren ebaluazioaren metrika honela osatzen da:

CVSS Oinarrizkoa: 9.1

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

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

CVE-2023-20855: kanpoko XML entitate (XXE) erako ahultasuna. Horren bitartez, vRealize Orchestrator-era sarbide ez administratzailea lukeen asmo gaiztoko eragile batek bereziki diseinatutako sarrerak erabil litzake XML analisien murrizpenak saihesteko, eta ondorioz informazio konfidentzialera sartzea edo pribilegioak eskalatzea lor liteke.

Ahultasunaren ebaluazioaren metrika honela osatzen da:

CVSS Oinarrizkoa: 8.8

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

- **Eraso bektorea: Sarea**
- **Erasoaren konplexutasuna: Baxua**
- **Behar diren pribilegioak: Baxuak**
- **Erabiltzailearekiko interakzioa: Batere ez**
- **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.

CVE-2023-20858 akats kritikoa konpontzeko VMwarek gomendatzen du bere oharrean eskuragarri dauden dagozkion segurtasun eguneraketak ezartzea:

- App Control-en 8.9.x bertsiorako Fixed bertsioa honako estekan eskuragarri.
- App Control-en 8.8.x bertsiorako Fixed bertsioa honako estekan eskuragarri.
- App Control-en 8.7.x bertsiorako Fixed bertsioa honako estekan eskuragarri.

CVE-2023-20855 ahultasunari dagokionez ere, VMwarek bere oharrean eskuragarri dauden segurtasun eguneraketak ezartzea gomendatzen du:

- VMware vRealize Orchestrator-erako Fixed Version honako estekan eskuragarri.
- VMware vRealize Automation-erako Fixed Version honako estekan eskuragarri.
- VMware Cloud Foundation-erako (vRealize Automation) Fixed Version honako estekan eskuragarri.

5. Erreferentzia Osagarriak

- VMSA-2023-0004.
- VMSA-2023-0005.
- CVE-2023-20855.
- CVE-2023-20858.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA