Basque CyberSecurity Centre

Kalteberatasunak - VMware vRealize Log Insight

BCSC-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

EDUKIAREN TAULA

Erantzukizunetik salbuesteko klausula

Erakundeen eta herritar interesdunen segurtasunaren mesedetan, BCSCk beharrezkotzat jotzen dituen alertak zabaltzeko helburua du honako 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 baldintzen araberako iritzi eta gomendioak dira, eta ezin da jakinarazitako informaziotik ondorio juridiko loteslerik atera.

Salmenta debekatzeko klausula

Erabat debekatuta dago dokumentu hau saltzea edo bere kontura edozein onura ekonomiko lortzea. Hala ere, ez zaio eragozpenik jarriko dokumentu hau kopiatzeko, banatzeko, hedatzeko edo zabaltzeko aukerari.

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 Gorabeherei 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-abisua

VMWare-k segurtasun-abisu bat argitaratu du VMware vRealize Log Insight produktuaren kalteberatasunak tratatzeko; horietako bi larritasun kritikoarekin kalifikatu dira, eta esleitutako CVSS 9.8 da. Tratatutako hutsegite-motak kodea urrunetik exekutatzea, informazioa zabaltzea eta zerbitzua ukatzea dira. Kalteberatasun horiei esleitutako identifikatzaileak hauek dira:CVE-2022-31706, CVE-2022-31704, CVE-2022-31710, CVE-2022-31711. Horien guztien kasuan eskuragarri dago segurtasun-eguneraketa bat, hutsegiteak tratatzen dituena eta haien inpaktua arintzen duena.

2. Eragindako baliabideak

- VMware vRealize Log Insight 8.x bertsioak

3. Analisi teknikoa

Eguneraketa horretan tratatutako kalteberatasunen xehetasunak hauek dira:

CVE-2022-31706: VMware vRealize Log Insight direktorioaren zeharkako kalteberatasuna; autentifikatu gabeko eragile gaizto batek fitxategiak injekta ditzake eragindako gailu baten sistema eragilean, eta horrek kodea urrunetik exekutatzeko aukera eman dezake.

Kalteberatasunaren metrika hau da:

CVSS Base: 9.8, kritikoa

CWE-94: Improper Control of Generation of Code (Code Injection)

CVE-2022-31704: sarbide-kontrolaren kalteberatasuna vRealize Log Insight-en; horrela, autentifikatu gabeko eragile gaizto batek fitxategiak injekta ditzake eragindako gailu baten sistema eragilean, eta horrek kodea urrunetik exekutatzeko aukera eman dezake.

Kalteberatasunaren metrika hau da:

CVSS Base: 9.8, kritikoa

CWE-94: Improper Control of Generation of Code (Code Injection)

CVE-2022-31710: vRealize Log Insight deserializatze-kalteberatasuna; horrela, autentifikatu gabeko eragile gaizto batek urrunetik eragin dezake konfiantzazkoak ez diren datuak deserializatzea, eta horrek zerbitzu-ukatzea eragin dezake.

Kalteberatasunaren metrika hau da:

CVSS Base: 7.5, handia

CWE-400: Uncontrolled Resource Consumption

CVE-2022-31711: informazioa zabaltzeko kalteberatasuna vRealize Log Insight-en. Eragile gaizto batek urrunetik bildu ahal izango du saioko eta autentifikaziorik gabeko aplikazioko informazio konfidentziala.

Kalteberatasunaren metrika hau da:

CVSS Base: 5.3, ertaina

CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

4. Arintzea / Konponbidea

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

Abisu honetan tratatutako kalteberatasunak arintzeko, VMWare-k segurtasun-eguneraketa bat argitaratu du; abisuan bertan kontsulta daiteke, eta esteka honetan eskuragarri dago.

5. Erreferentzia gehigarriak

- VMWare
- Segurtasun-abisua
- VMware vRealize Log Insight
- CVSS
- Kodearen urruneko exekuzioa
- Informazioa zabaltzea
- Zerbitzua ukatzea
- CVE-2022-31706
- CVE-2022-31704
- CVE-2022-31710
- CVE-2022-31711

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA