Basque CyberSecurity Centre

Kalteberatasunak - Citrix Hypervisor (CVE-2022-3643, CVE-2022-42328, CVE-2022-42329)

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

Citrix-ek 3 akats konpontzen dituen segurtasun-eguneraketa bat argitaratu du (Citrix Hypervisor 8.2 LTSR CU1), CVE-2022-3643, CVE-2022-42328 CVE-2022-42329identifikatzaileekin. Lehenengoa larritasun kritikoarekin kalifikatu da, eta 10.0.ko CVSSarekin. Horiek guztiek aukera eman dezakete erabiltzaile pribilegiatu batek gonbidatutako makina birtual batean ostalariak erantzuteari uztea edo blokeatzea eragiteko.

2. Eragindako baliabideak

- Citrix Hypervisor 8.2 LTSR CU1

3. Analisi teknikoa

CVE-2022-3643 gisa identifikatutako kalteberatasuna bat dator guest erabiltzaileek netback bidez NIC interfazea berrabiaraztea/abortatzea/blokeatzea aktiba dezaketen hutsegite batekin. Baliteke guest erabiltzaile batek NIC interfazea Linux-en oinarritutako sareko backend batean berrabiaraztea/abortatzea/blokeatzea aktibatzea, zenbait pakete-mota bidaliz. Jakinarazi da hori hauekin gertatzen dela: Cisco (enic) eta Broadcom NetXtrem II BCM5780 (bnx2x); baina baliteke arazoa bestelako NIC/kontrolagailu batzuekin ere sortzea. Interfazeak goiburu zatituak dituzten eskaerak bidaltzen baditu, netback-ak sarearen nukleora birbidaliko ditu lehen aipatutako suposizioa urratzen dutenak, eta horrek portaera txar hori eragingo du.

Kalteberatasunaren metrika:

CVSS Base: 10.0, kritikoa

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

- **Eraso-bektorea: Sarea**
- **Erasoaren konplexutasuna: Txikia**
- **Eskatutako pribilegioak: Bat ere ez**
- **Erabiltzailearekiko interakzioa**: **Bat ere ez**
- **Irismena: Aldaketekin**
- **Konfidentzialtasuna: Handia**
- **Osotasuna: Handia**
- **Erabilgarritasuna: Handia**

CVE-2022-42328 kalteberatasunari dagokionez, hutsegite horrek aukera ematen du guest erabiltzaileek elkar-blokeatzeak eragin ahal izateko Linuxeko netback kontrolagailuan.

Kalteberatasunaren metrika:

CVSS Base: 5.3, ertaina

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

- **Eraso-bektorea:** Lokala
- **Erasoaren konplexutasuna: Txikia**
- **Eskatutako pribilegioak:** Txikiak
- **Erabiltzailearekiko interakzioa**: **Bat ere ez**
- **Irismena:** Aldaketarik gabe
- **Konfidentzialtasuna:** Bat ere ez
- **Osotasuna:** Bat ere ez
- **Erabilgarritasuna: Handia**

Azkenik, CVE-2022-42329 hutsegiteak, aurrekoak bezala, aukera ematen du guest erabiltzaileek elkar-blokeatzeak eragin ahal izateko Linuxeko netback kontrolagailuan.

Kalteberatasunaren metrika:

CVSS Base: 5.5, ertaina

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

- **Eraso-bektorea:** Lokala
- **Erasoaren konplexutasuna: Txikia**
- **Eskatutako pribilegioak:** Txikiak
- **Erabiltzailearekiko interakzioa**: **Bat ere ez**
- **Irismena:** Aldaketarik gabe
- **Konfidentzialtasuna:** Bat ere ez
- **Osotasuna:** Bat ere ez
- **Erabilgarritasuna: Handia**

4. Arintzea / Konponbidea

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

Horregatik, Citrix-ek berrikuspen bat eskaini du arazo horiek konpontzeko. Citrix-ek gomendatzen du eragindako bezeroek berrikuspen hori instalatzea, eguneraketak aplikatzeko programak ahalbidetzen dienaren arabera. Berrikuspena esteka honetatik deskarga daiteke:

Citrix Hypervisor 8.2 LTSR CU1: CTX476080

5. Erreferentzia gehigarriak

- CVE-2022-3643
- CVE-2022-42328
- CVE-2022-42329
- Citrix-en segurtasun-eguneraketa
- Citrix Hypervisor 8.2 LTSR CU1
- Hotfix Citrix Hypervisor 8.2 LTSR CU1: CTX476080

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA