Basque CyberSecurity Centre

Citrix Gateway eta Citrix ADC (CVE-2022-27510, CVE-2022-27513, CVE-2022-27516)

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 segurtasun-buletin bat argitaratu du, eta bertan adierazi du kalteberatasunak aurkitu dituztela Citrix Gateway-n eta Citrix ADC-n CVE-2022-27510, CVE-2022-27513 eta CVE-2022-27516 identifikatzaileekin, eta haietako lehena larritasun kritikokoa dela (CVSS: 9.8).

2. Eragindako baliabideak

- Citrix ADC eta Citrix Gateway 13.1, 13.1-33.47 bertsioaren aurrekoa
- Citrix ADC eta Citrix Gateway 13.0, 13.0-88.12 bertsioaren aurrekoa
- Citrix ADC eta Citrix Gateway 12.1, 12.1.65.21 bertsioaren aurrekoa
- Citrix ADC 12.1-FIPS, 12.1-55.289 bertsioaren aurrekoa
- Citrix ADC 12.1-NDcPP, 12.1-55.289 bertsioaren aurrekoa

3. Analisi teknikoa

Hona hemen eguneraketa honetan landutako kalteberatasunak:

CVE-2022-27510: Gateway-ko erabiltzailearen gaitasunetan baimendu gabe sartzean datzan kalteberatasuna.

Kalteberatasuna ebaluatzeko metrika honela dago osatuta:

Oinarrizko CVSS: 9.8

CWE-288: Autentikazioa bide edo kanal alternatibo baten bidez bideratzea

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

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

CVE-2022-27513: urruneko mahaigainaren kontrola *phishing* bidez hartzean datzan kalteberatasuna

Kalteberatasuna ebaluatzeko metrika honela dago osatuta:

Oinarrizko CVSS: 8.3

CWE-345: Datuen benetakotasunaren egiaztapen eskasa

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

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

CVE-2022-27516: erabiltzailearen saio-hasierako indar handiko babesaren funtzionaltasunari eragiten dion kalteberatasuna.

Kalteberatasuna ebaluatzeko metrika honela dago osatuta:

Oinarrizko CVSS: 5.3

CWE-693: Babes-mekanismoaren hutsegitea

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

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

4. Arintzea / Konponbidea

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

Citrix-ek hau gomendatzen die Citrix ADCren eta Citrix Gateway-ren eragindako bezeroei: Citrix ADCren edo Citrix Gateway-ren bertsio eguneratuak lehenbailehen instala ditzatela. Hauek dira eragindako bertsioak:

- Citrix ADC eta Citrix Gateway 13.1-33.47 eta ondorengo bertsioak
- Citrix ADC eta Citrix Gateway 13.0-88.12 eta 13.0 bertsioaren ondorengoak
- Citrix ADC eta Citrix Gateway 12.1-65.21 eta 12.1 bertsioaren ondorengoak
- Citrix ADC 12.1-FIPS 12.1-55.289 eta 12.1-FIPS bertsioaren ondorengoak
- Citrix ADC 12.1-NDcPP 12.1-55.289 eta 12.1-NDcPP bertsioaren ondorengoak

Horrez gain, eta aipatutako CVEekin loturarik izan gabe, segurtasun-hobekuntzak gehitu dira, bezeroak HTTP eskaeren kontrabando-erasoetatik hobeto babesteko, Citrix ADCren eta Citrix Gateway-ren aurreko bertsioetan. Bezeroek Citrix ADCren administrazio-interfazearen bidez ezar ditzakete hobekuntza horiek. Webgune honetan kontsulta daitezke: https://support.citrix.com/article/CTX472830/citrix-adc-http-request-smuggling-reference-guide.

5. Erreferentzia gehigarriak

- Citrix-en segurtasun-buletina
- CVE-2022-27510
- CWE-288
- CVE-2022-27513
- CWE-345
- CVE-2022-27516
- CWE-693
- https://support.citrix.com/article/CTX472830/citrix-adc-http-request-smuggling-reference-guide

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA