Basque CyberSecurity Centre

# Kalteberatasunak - Zyxel firmware NR7101 (CVE-2022-43389, CVE-2022-43390, CVE-2022-43391, CVE-2022-43392)

BCSC-ABISUAK

**TLP: CLEAR**

www.zibersegurtasun.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

# EDUKIEN TAULA



## Erantzukizunetik salbuesteko klausula

Dokumentu hau ematen da BCSCk erakundeen eta herritar interesdunen segurtasunaren alde beharrezkotzat jotzen dituen alertak zabaltzeko. 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

## 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-oharra

Zyxel-ek segurtasun-abisu bat argitaratu du. Bertan, komandoak injektatzeko eta CPEren, zuntzaren ONTren eta WiFi hedagailuen bufer-gainezkatzearen 4 kalteberatasun azaltzen dira. CVE-2022-43389, CVE-2022-43391 eta CVE-2022-43392 hutsegiteek larritasun handia dute; CVE-2022-43390 hutsegiteak, berriz, ertaina.

Kalteberatasun horiek eragiten duten inpaktu nagusia –eguneratzen ez badira– bat dator eragindako osagaien erabilgarritasuna galtzearekin, kalteberatasunak arrakastaz ustiatuz gero.

## 2. Eragindako baliabideak

- NR7101 firmwarearen mendeko produktuak V1.15 (ACCC.3) C0 baino lehenagoko bertsioetan

## 3. Analisi teknikoa

Hona hemen tratatutako kalteberatasunen xehetasunak:

CVE-2022-43389: web-zerbitzariaren liburutegian bufer-gainezkatzearen kalteberatasuna Zyxel NR7101 firmwarean eta V1.15 (ACCC.3) C0 baino lehenagoko bertsioetan, aukera eman diezaiokeena autentifikatu gabeko erasotzaile bati sistema eragileko komando batzuk exekutatzeko edo zerbitzua ukatzeko baldintzak (DoS) eragiteko gailu kaltebera batean.

Kalteberatasunaren metrika hau da:

CVSS Base: 8.6, handia

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

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

CVE-2022-43391: bufer-gainezkatzearen kalteberatasuna CGI programaren parametroan V1.15 (ACCC.3) C0 baino lehenagoko Zyxel NR7101 firmwarean; aukera eman dezake autentifikatutako erasotzaile batek zerbitzua ukatzeko baldintzak (DoS) eragiteko manipulatutako HTTP eskaera bat bidaliz.

Kalteberatasunaren metrika hau da:

CVSS Base: 7.1, handia

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

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

CVE-2022-43392: bufer-gainezkatzearen kalteberatasuna web-zerbitzariaren parametroan V1.15 (ACCC.3) C0 baino lehenagoko Zyxel NR7101 firmwarean; aukera eman dezake autentifikatutako erasotzaile batek zerbitzua ukatzeko baldintzak (DoS) eragiteko manipulatutako baimen-eskaera bat bidaliz.

Kalteberatasunaren metrika hau da:

CVSS Base: 7.1, handia

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

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

CVE-2022-43390: komandoak injektatzeko kalteberatasuna V1.15 (ACCC.3) C0 baino lehenagoko Zyxel NR7101 firmwarearen CGI programan; aukera eman dezake autentifikatutako erasotzaile batek sistema eragileko komando batzuk exekutatzeko gailu kaltebera batean, manipulatutako HTTP eskaera bat bidaliz.

Kalteberatasunaren metrika hau da:

CVSS Base: 5.4, ertaina

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

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

## 4. Arintzea / Konponbidea

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

Zyxel-ek erabiltzaileei gomendatzen die egoki diren firmware-eguneraketak instala ditzatela; eguneraketa horien zerrenda segurtasun-oharrean kontsulta daiteke, babes optimoa lortzeko. Halaber, adierazten da deskarga-estekarik ez duten produktuen kasuan bezeroek Zyxel-en laguntza lokaleko zerbitzuko lantaldearekin harremanetan jarri behar dutela artxiboa lortzeko. Azkenik, jakinarazten da ISP batetik datorren Zyxel gailua jaso zuten azken erabiltzaileen kasuan gomendatzen dela zuzenean ISParen laguntza-zerbitzuko lantaldearekin harremanetan jartzea, gailuak konfigurazio pertsonalizatuak izan baititzake.

## 5. Erreferentzia gehigarriak

- Zyxel-en segurtasun-abisua
- CVE-2022-43389
- CVE-2022-43391
- CVE-2022-43392
- CVE-2022-43390


EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA