



Ahultasuna Zykel-en biltegitratze gailuetan (NAS)

BCSC-OHARRAK

TLP: CLEAR

www.zibersegurtasun.eus



AURKIBIDEA

BCSCri buruz.....	3
1. Segurtasun oharra.....	4
2. Kaltetutako baliabideak	5
3. Azterketa teknikoa	6
4. Arintzea / Konponbidea	7
5. Erreferentzia Osagarriak.....	8

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, ustekabeen 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

Gutziz debekatuta dago dokumentu hau saltzea edo beragatik edozein onura ekonomiko eskuratzea, baina posible da bera kopiazea, banatzea, hedatzea edo ezagutzera ematea.

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 erreferentziatzeko 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 jardura dinamizatzea eta erreferentzia izango den sektore profesional bat sor dadin eragitea. Testuinguru horretan osagarriak diren eragileen arteko lankidetzak proiektuak exekutatzeko 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 analisisian, eta euskal gizartearen beharrak artatzeko beharrezkoak diren prebentzio neurrien diseinuan. Helburu horiek lortzeko xedearekin, zibersegurtasun gertakariak kudeatzera zuzendutako hainbat ekimenetan hartzen du parte:



1. Segurtasun oharra

Zyxelek [segurtasun ohar](#) bat argitaratu du, sarean konektatutako biltegiatze gailu batzuei (NAS) eragiten dien ahultasun bat zuzentzen duena. Modelo horiek Zyxel [NAS326](#), [NAS540](#) eta [NAS542](#) dira. Akatsa larritasun altukoa da eta [CVE-2023-27988](#) identifikatzailea dauka. Horrek komandoen injekzio erako egoera eragin lezake urrunetik sistema eragilean. Ustiatua izanez gero sistemen konfidentzialtasun, integritate eta eskuragarritasunean inpaktu altua eragingo litzateke.

Fabrikatzaileak dagoeneko argitaratu du nabarmendutako akatsa konpontzen duen eguneraketa. Horregatik, ahultasun hau eta beste batzuk prebenitzeko gomendatzen da sistemak eta aplikazioak beti eguneratuta izatea.

2. Kaltetutako baliabideak

- Zyxel NAS326, V5.21(AAZF.12)C0 eta lehenagoko bertsioak.
- Zyxel NAS540, V5.21(AATB.9)C0 eta lehenagoko bertsioak.
- Zyxel NAS542, V5.21(ABAG.9)C0 eta lehenagoko bertsioak.

3. Azterketa teknikoa

Ohar honetan aztertutako ahultasunaren xehetasunak honakoak dira:

CVE-2023-27988: autentifikazioaren ondoren komandoen injekzio erako ahultasuna. Hori baliatuz autentifikatutako erasotzaile batek, administratzaile pribilegioak baldin baditu, sistema eragileko komando batzuk exekuta litzake urrunetik kaltetutako gailu batean.

Ahultasunaren ebaluazioaren metrika honela osatzen da:

CWE 78: Improper Neutralization of Special Elements used in an OS Command (OS Command Injection)

CVSS Base: 7.2

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

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

4. Arintzea / Konponbidea

Ahultasun hau arintzeko gomendatzen da sistemak eta aplikazioak beti eguneratuta izatea eskuragarri dagoen azken bertsiora, dagozkion eguneraketak argitaratu bezain azkar.

Ohar honetan aztertutako akatsa zuzentzeko, Zyxelek firmware eguneraketak argitaratu ditu kaltetutako modeloetarako, ondorengo esteketan eskuragarri daudenak:

- [Zyxel NAS326 gailurako eguneraketa](#).
- [Zyxel NAS540 gailurako eguneraketa](#).
- Zyxel [NAS542](#) gailuetarako eguneraketa [oharraren](#) barnean bertan dago eskuragarri zuzeneko deskarga modura.

5. Erreferentzia Osagarriak

- Segurtasun oharra.
- CVE-2023-27988.

 Basque
CyberSecurity
Centre