Basque CyberSecurity Centre

Ahultasun kritikoak Zyxel-en ZyWall firewall-etan

BCSC-OHARRAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

AURKIBIDEA

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, ustekabean 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

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

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Segurtasun oharra

Zyxelek gida bat argitaratu du ZyWall gailuen aurka berriki egin diren erasoekin zerikusia duten arazoei aurre egiteko eta horien eragina arindu ahal izateko. Erasotzaileak erabiltzen ari diren ahultasunak CVE-2023-28771, CVE-2023-33009 eta CVE-2023-33010 dira. Ahultasun horiek ustiatuz gero kodearen urruneko exekuzioa eta zerbitzuaren ukapena eragin litezke, eta horrek mehatxu nabarmena suposatuko luke kaltetutako sistemen konfidentzialtasun, integritate eta eskuragarritasunerako.

Fabrikatzaileak dagoeneko argitaratu ditu nabarmendutako akatsak konpontzen dituzten eguneraketak. Horregatik, ahultasun hau eta beste batzuk prebenitzeko gomendatzen da sistemak eta aplikazioak beti eguneratuta izatea.

2. Kaltetutako baliabideak

Kaltetutako produktuak	CVE-2023- 28771-ren kasuan kaltetutako bertsioak	CVE-2023- 33009 eta CVE-2023-33010-en kasuetan kaltetutako bertsioak
ATP	ZLD, V4.60 bertsiotik V5.35 bertsiora bitartekoak	ZLD, V4.32 bertsiotik V5.36 Patch 1 bertsiora bitartekoak
USG FLEX	ZLD, V4.60 bertsiotik V5.35 bertsiora bitartekoak	ZLD, V4.50 bertsiotik V5.36 Patch 1 bertsiora bitartekoak
USG FLEX50(W) / USG20(W)-VPN	Ez dagokio	ZLD, V4.25 bertsiotik V5.36 Patch 1 bertsiora bitartekoak
VPN	ZLD, V4.60 bertsiotik V5.35 bertsiora bitartekoak	ZLD, V4.30 bertsiotik V5.36 Patch 1 bertsiora bitartekoak
ZyWALL/USG	ZLD, V4.60 bertsiotik V4.73 bertsiora bitartekoak	ZLD, V4.25 bertsiotik V4.73 Patch 1 bertsiora bitartekoak

3. Azterketa teknikoa

Ohar honetan aztertutako ahultasunen xehetasunak honakoak dira:

CVE-2023-28771: firewall-aren bertsio batzuetan errore mezuen erabilpen okerra eragiten duen ahultasuna. Hori baliatuz autentifikatu gabeko erasotzaile batek sistema eragilearen komandoak exekuta litzake urrunetik, kaltetutako gailu batera manipulatutako paketeak bidaliz.
Ahultasunaren ebaluazioaren metrika honela osatzen da:

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

CVSS Base: 9.8

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

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

CVE-2023-33009: bufferraren gainezkatze erako ahultasuna firewall-aren bertsio batzuetako jakinarazpen funtzioan. Hori baliatuz autentifikatu gabeko erasotzaile batek zerbitzuaren ukapen egoerak (DoS) eragin litzake eta baita urrunetik kodea exekutatu ere kaltetutako gailu batean.

Ahultasunaren ebaluazioaren metrika honela osatzen da:

CWE 120: Buffer Copy without Checking Size of Input (Classic Buffer Overflow)

CVSS Base: 9.8

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

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

CVE-2023-33010: bufferraren gainezkatze erako ahultasuna firewall-aren bertsio batzuetako IDaren prozesamendu funtzioan. Hori baliatuz autentifikatu

gabeko erasotzaile batek DoS egoerak eragin litzake eta baita urrunetik kodea exekutatu ere kaltetutako gailu batean.

Ahultasunaren ebaluazioaren metrika honela osatzen da:

CWE 120: Buffer Copy without Checking Size of Input (Classic Buffer Overflow)

CVSS Base: 9.8

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

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

4. Arintzea / Konponbidea

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

Alde batetik, Zyxelek ezagutzera eman ditu gailuak kaltetuta daudela adieraz dezaketen sintomak, honakoak dira:

- Gailuak erantzuteari utzi dio.
- Ezin da gailuaren web kudeaketako interfazera edo SSHra sartu.
- Etenak sarean.
- VPN konexioen deskonexioak.

Bestalde, aipatutako ahultasunak konpontzeko, Zyxelek erabiltzaileei biziki gomendatzen die eskuragarri dagoen firmwarearen azken bertsioa instalatzea, konpainiak erabiltzen dituen ohiko kanalen bidez (gailu lokalen kasuan web interfazeko push jakinarazpenen bitartezko eguneraketa eta hodeian oinarritutako gailuen kasuan firmwarearen eguneraketa programatuak), akatsak zuzentzearren eta babes egokia bermatzearren. Gainera, ondorengo urratsak jarraitzea gomendatzen da, aldi baterako arintze eta arreta neurri modura:

- Gailuak WANaren aldetik administratzea guztiz beharrezkoa ez bada, WANeko HTTP/HTTPS zerbitzuak desgaitzea gomendatzen da.

Gailuak WANaren aldetik kudeatzea beharrezkoa bada:

- Politiken Kontrola gaitzea eta arauak gehitzea, sarbidea soilik fidagarriak diren sortze IP helbideetatik baimentzeko.
- GeoIP iragazkia gaitzea, sarbidea soilik fidagarriak diren kokapenetatik baimentzeko.
- VPN IPSec-en funtzioa erabili behar ez bada, UDP 500 eta 4500 atakak desgaitzea.

5. Erreferentzia Osagarriak

- Zyxel ZyWall gida.
- CVE-2023-28771.
- CVE-2023-33009.
- CVE-2023-33010.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA