Basque CyberSecurity Centre

# Ahultasun kritikoa WooCommerce Payments-en

**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

# BCSC-ri 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. Era berean, Eusko Jaurlaritzako beste hiru Sail ere bere parte dira: Segurtasuna, Gobernantza Publiko eta Autogobernua, eta Hezkuntza; bai eta Zientzia, Teknologia eta Berrikuntzako Euskal Sistemako lau eragile 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, ingeleseko 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. Laburpen exekutiboa

Wordfence-k, WordPress-eko segurtasun analistek osatutako taldeak, segurtasun iragarki bat jarri du martxan. Bertan ahultasun bat nabarmentzen da, eta larritasun kritikoz katalogatu da. Akats horrek *WooCommerce Payments* pluginari eragiten dio, 500.000 deskarga baino gehiago baititu.

Oraingoz ez du CVE identifikatzailerik esleituta, baina, akats horren ondorioz, kautotu gabeko erasotzaile batek *WooCommerce Payments-en* bertsio kaltebera duten dendetan administratzaile baimena eskuratu dezake.

Azpimarratzekoa da Wordfence-k baieztatu duela, oraingoz, ez dela hauteman mehatxu eragileak ahultasun hori aktiboki ustiatzen ari direnik. Aldiz, eskala handiko erasoak espero dira kontzeptu-proba (PoC) jendaurrean ikusgai dagoenean.

Fabrikatzaileak dagoeneko argitaratu du dagokion eguneratzea, eta horrela akats kritiko nabarmena zuzendu du. Horregatik, ahultasun horiei eta beste batzuei aurrea hartzeko, sistemak eta aplikazioak erabilgarri dagoen azken bertsioan eguneraturik izatea gomendatzen da.

## 2. Azterketa teknikoa

Wordfence-k emandako ahultasun kritikoari dagokionez, nabarmendu behar da CVSSv3 eskalan 9,8ko puntuazioa duela. Ahultasun horri buruzko xehetasun askorik eman ez den arren, badakigu badagoela, *determine current user for platform checkout* funtzioan kautotzea falta delako. Akats horren ondorioz, autentifikatu gabeko urruneko erasotzaile batek edozein erabiltzaileren identitatea ordezteko gaitasuna hartzen du, eta pribilegioen eskalada egiten du. Horretarako, ukitutako osagarriaren bertsio ahula duen denda bateko administratzailearen baimenak lortzen ditu kontuan.

Lehen deskribatutako ahultasuna ebaluatzeko metrikak honela osatzen dira:

CVSS Oinarria: 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: Txikia**
- **Beharrezko pribilegioak: Bat ere ez**
- **Erabiltzailearekiko interakzioa: Bat ere ez**
- **Irismena:** Aldaketarik ez
- **Konfidentzialtasuna: Altua**
- **Osotasuna: Altua**
- **Erabilgarritasuna: Altua**

Azkenik, aurreko ahultasunak bertsio hauei eragiten die:

- *WooCommerce Payments* 5.6.1 bertsioa eta aurrekoak, 4.8.2, 4.9.1, 5.0.4, 5.1.3, 5.2.2, 5.3.1, 5.4.1 eta 5.5.2 izan ezik.

## 3. Arintzea / Konponbidea

Ohiko moduan, ahultasun horiei eta beste batzuei aurrea hartzeko, sistemak eta aplikazioak eskuragarri dagoen azken bertsiora eguneratuta izatea gomendatzen da, eguneratzeak argitaratu bezain laster.

Horretarako, *WooCommerce Payments* plugina 5.6.2 bertsiora eguneratu behar da.

Horrez gain, fabrikatzaileak eman beharreko pauso hauek eman ditu ukitutako osagarria eskuz eguneratzeko:

- Lehenik eta behin, administratzaileek WordPress-en administrazio panelera sartu behar dute, *Plugins-en menuan* sartuz eta zerrendan *WooCommerce Payments* bilatuz.
- *Deskribapena* zutabean, instalatutako bertsioa agertzen da. Bertsio ahulik ez badago, ez da ezer egin behar.
- Bertsio ahul bat izanez gero, WooCommerce Payments osagarriaren 5.6.2 bertsioa eguneratzeko aukera ematen duen ohar erabilgarrira sartu behar da.

Horrez gain, fabrikatzaileak erabiltzaileei eskatzen die eragindako pluginaren 5.6.2 bertsioa ezar dezatela, eta horrela ustiapenari aurrea har diezaiotela bai ahultasun nabarmenari bai etorkizuneko akatsei.

## 4. Erreferentzia osagarriak

- Wordfence.
- WordPress.
- PSA: Update Now! Critical Authentication Bypass in WooCommerce Payments Allows Site Takeover.
- WooCommerce Payments.
- WordPress force patching WooCommerce plugin with 500K installs.
- WooCommerce Payments <= 5.6.1 Authentication Bypass and Privilege Escalation.
- CWE-862: Missing Authorization.


EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA