Basque CyberSecurity Centre

WordPress-en ahultasunak

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

Wordfencek, WordPress-eko segurtasun analistek osatutako taldeak, segurtasun iragarki bat kaleratu du. Iragarki horretan 3 ahultasun nabarmentzen dira, horietako bi zorroztasun kritikoarekin katalogatuta, eta horietako bat kritikotasun handiarekin puntuatuta. Akats horiek plugin desberdinei eragiten diete, milaka deskarga baitituzte, eta Paid Memberships Pro, Easy Digital Downloads eta Survey Maker izenez ezagutzen dira.

Lehenik eta behin, CVE-2023-23488an identifikatutako ahultasun bat erantsi da, eta zorrotz kalifikatu du fabrikatzaileak. Errore horri esker, urruneko erasotzaile batek SQL kodea injektatu dezake sistema kalteberan.

Jarraian, nabarmendu behar da CVE-2023-234889ren pean erregistratutako eta fabrikatzaileak zorroztasun kritikoz katalogatutako ahultasuna. Aurreko kasuan bezala, urrakortasun horrek urruneko erasotzaile bati SQL kodea injektatzea ahalbidetzen dio sistema kalteberan.

Azkenik, CVE-2023-23490aren pean erregistratutako eta fabrikatzaileak larritasun handiarekin katalogatutako ahultasuna SQL kodea gailu kaltebera batean injektatzean gerta daiteke.

Azpimarratzekoa da Joshua Martinelle ikertzaileak akats horien berri emateaz gain, ahultasun bakoitzeko kontzeptu proba bat (PoC) argitaratu duela. Halaber, gaur egun ez dakigu akats horiek sarean aktiboki ustiatu direla.

Fabrikatzaileak dagoeneko argitaratu ditu dagozkion adabakiak, akats nabarmenak zuzentzeko. Beraz, ahultasun horiei eta beste batzuei aurrea hartzeko, BCSCk gomendatzen du sistemak eta aplikazioak eguneratuta izatea eskura dagoen azken bertsioan, dagozkion adabakiak argitaratu bezain laster.

2. Azterketa teknikoa

Lehenik eta behin, *Paid Memberships Pro* pluginari eragiten dion CVE-2023-23488-ren pean erregistratutako ahultasuna akats bat da, */pmpro/v1/order REST* bideko code parametroaren akats baten ondorioz gertatzen dena, eta urruneko erasotzaile batek SQL kodea injektatzeko aukera ematen du. Horrela, kautotu gabeko zibererasotzaileek SQL kontsultak gehitu ditzakete, eta informazio konfidentziala atera dezakete eragindako datu-basetik.

Akats hori argitaratutako kontzeptu probaren arabera ustiatzeko, mehatxu aktore batek SLEEP funtzioa erabil dezake plugin ahultasunaren WordPress-en ostalariaren helbidean. Ekintza horrek atzerapena ekarriko du egindako eskaeraren itzuleran. Hona hemen argitaratutako kontzeptu-proba:

```
curl
"http://TARGET_HOST/?rest_route=/pmpro/v1/order&code=a%27%20OR%20(SELECT%201%20FROM%20
(SELECT(SLEEP(2)))a)--%20-"
```

1. irudia PoC del CVE-2023-23488

Bigarren ahultasuna CVE-2023-234889-ren bidez identifikatu da eta *Easy Digital Downloads* pluginari eragiten dio. Horri esker, SQL kodea injekta daiteke AJAX *edd_downloadsearch* lanean erabilitakos parametroaren bidez. Aurreko ahultasunean bezala, akats hori arrakastaz ustiatzeak arriskuan dagoen datu-basetik informazio konfidentziala ateratzea ekarriko luke.

Oraingoan, argitaratutako kontzeptu-probaren arabera, aurreko kasuan bezala aprobetxa daiteke ahultasun hori. Hala ere, nabarmendu behar da SQL injekzio bakarra ezin izango dela bi aldiz jarraian egin, *edd_ajax_download_search()* funtzioak hogeita hamar segundoz egindako bilaketak biltegiratzen baititu; beraz, karga erabilgarri bera ezartzeko, pixka bat aldatu beharko da edo erasotzaileak hogeita hamar segundoz itxaron beharko du.

```
curl
"http://TARGET_HOST/wp-admin/admin-ajax.php?action=edd_download_search&s=1'+AND+(SELEC
T+1+FROM+(SELECT(SLEEP(2)))a)--+-"
```

2. irudia PoC del CVE-2023-23489

Hirugarren ahultasuna, CVE-2023-23490-ren pean erregistratua eta *Survey Maker* pluginari eragiten diona, SQL kodea injekta daitekeelako AJAX *ays_surveys_export_json*-en ekintzaren bidez. Ekintza honen bidez, erasotzaile kautotu bati edo harpidedun pribilegioak dituen bati informazioa kontsultatu eta dagokion datu-basetik ateratzeko aukera ematen zaio.

Argitaratutako kontzeptu probaren arabera, curl komando sinplea erabil daiteke ahultasuna ustiatzeko, baina baliozko saio cookie bat behar da. Akats hori aprobetxatzeko, mehatxu-aktore batek *$TARGET_HOST* ordezkatu behar du WordPress eta *$WP_COOKIE* helmuga-instantzia batekin, saioa hasi duen erabiltzaile batentzat.

```
curl "http://$TARGET_HOST/wp-admin/admin-ajax.php" --header "$WP_COOKIE" --data
"action=ays_surveys_export_json&surveys_ids[0]=1)+AND+(SELECT+1+FROM+(SELECT(SLEE
P(3)))a)--+-"
```

3. irudia PoC del CVE-2023-23490

Azkenik, ahultasun horiek produktu hauei eragiten diete:

- *Paid Memberships Pro* 2.9.8 bertsioaren aurrekoak.
- *Easy Digital Downloads* 3.1.0.4 bertsioaren aurrekoak.
- *Survey Maker* 3.1.2 bertsioaren aurrekoak.

3. Arintzea / Konponbidea

Ohiko moduan, ahultasun hori eta beste batzuk saihesteko, BCSCk gomendatzen du sistemak eta aplikazioak beti eguneratuta izatea eskura dagoen azken bertsiora, dagozkion adabakiak argitaratu bezain laster.

Garrantzitsua da neurriak azkar hartzea, inplementazioko arazo horiek arintzeko. Horregatik, fabrikatzaileek proposatutako irtenbide ofizialak aplikatzea gomendatzen da.

CVE-2023-23488 ahultasunari dagokionez, erabiltzaileek *Paid Memberships Pro* plugina 2.9.8 bertsiora eguneratu behar dute, esteka honen bidez:

- https://wordpress.org/plugins/paid-memberships-pro

CVE-2023-234889 ahultasunari dagokionez, fabrikatzaileak *Easy Digital Downloads* plugina 3.1.0.4 bertsiora eguneratzea eskatu du. Esteka honetan dago eskuragarri:

- https://wordpress.org/plugins/easy-digital-downloads/

Azkenik, CVE-2023-23490 kodearekin identifikatutako akatsa konpontzeko, WordPress-ek *Survey Maker* plugina 3.1.2 bertsiora eguneratzea gomendatzen du, esteka honen bidez:

- https://wordpress.org/plugins/survey-maker

4. Erreferentzia osagarriak

- Wordfence.
- Wordfence Intelligence Community Edition.
- Paid Memberships Pro plugin.
- Easy Digital Downloads plugin.
- Survey Maker plugin.
- Paid Memberships Pro < 2.9.8 - SQL Injection.
- Easy Digital Downloads < 3.1.0.4 - SQL Injection.
- Survey Maker < 3.1.2 - Authenticated SQL Injection.
- MITRE: CVE-2023-23488.
- MITRE: CVE-2023-234889.
- MITRE: CVE-2023-23490.
- Tenable: Joshua Martinelle.
- SQL Injection in Multiple WordPress Plugins.
- PoC exploits released for critical bugs in popular WordPress plugins.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA