Zimbra zero-day Ahultasuna

BCSC-AHULTASUNA- ZIMBRA-ZERO-DAY

TLP:WHITE

www.basquecybersecurity.eus

2022ko Otsaila

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, 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:

1. LABURPEN EXEKUTIBOA

2021eko abenduan, Volexity zibersegurtasun enpresak phishing kanpaina batzuk identifikatu zituen bezero baten aurka. Emandako datuekin, ezin izan zaio esleitu maltzurkeriazko jarduera aldez aurretik ezagutzen den mehatxu-aktore bati. Hala ere, behatutako faktore batzuetan oinarrituta, Volexityk dio litekeena dela erasotzailea txinatar jatorrikoa izatea, TEMP_Heretic izenekoa. Ahultasun horren aurkikuntzak garrantzi handia du, 200.000 enpresatan eta gobernu eta finantza-erakundeetan baino gehiagotan dagoen softwarea baita.

Kanpaina horietako mezu elektronikoak aztertu ondoren, segurtasun ikertzaileek ikusi zuten Zimbran (kode irekiko posta elektronikoko plataforma bat, erakundeek Microsoft Exchange-ren ordezko gisa erabiltzen dutena) zero eguneko leku gurutzatuetan (XSS) komando-sekuentziaren ahultasuna ustiatzen ari zirela.

Phishing-kanpainak bi etapatan egin ziren: lehenengoa, aintzatespen-fasea zen, eta helburua zen biktimek mezuak jaso eta ireki zituzten arakatzea eta baieztatzea. Bigarren etapan, biktimak engainatu egiten ziren, erasotzaileek sortutako mezu batean jasotako iruzurrezko esteka batera sar zitezen. Erasoak arrakasta izan zezan, beharrezkoa zen biktimak hitzartutako esteka bisitatzea Zimbraren web postara web nabigatzaile batetik konektatuta zegoen bitartean.

Eraso horien helburu nagusia erabiltzailearen postako datu eta fitxategi erantsiak lapurtzea zen. Gainera, ahultasunaren ondorioz, erasotzaileak erraz egin ditzake beste ekintza batzuk erabiltzailearen saioaren testuinguruan; adibidez, cookieak iragaztea postontzi batera etengabe sartzeko, phishing-mezuak bidaltzea biktimaren postontzitik edo ohar bat aurkeztea kode kaltegarria deskargatzeko konfiantzako web gune baten testuinguruan.

Fabrikatzailearen webgunetik egiaztatu da ahultasunak Zimbrari (8.8.15) eta aurreko bertsioei eragiten diela. Gaur egun, ez dago adabaki erabilgarririk, ez eta ahultasun horretarako CVErik ere. Konpainiak oraindik adabaki ofizialik ez duenez, Zimbraren softwarea bertsio berrienera (9.0.0 bertsioa) eguneratzea gomendatzen zaie erabiltzaileei. Zimbraren erabiltzaileek datu historikoak aztertu behar dituzte sarbide susmagarriak bilatzeko.

2. AZTERKETA TEKNIKOA

Volexityk aurkitutako ahultasuna, oraindik CVE bakar baten pean katalogatu ez dena, Zimbra kode irekiko posta elektronikoko plataformari eragiten dion zero-eguneko gune gurutzatuetako komando-sekuentzien (XSS) ahultasun gisa definitu da. Ahultasun horren ustiapen arrakastatsuak, besteak beste, JavaScript kode arbitrarioa exekutatzeko aukera eman dezake Zimbraren erabiltzailearen saioaren testuinguruan.

Volexityko ikertzaileek jakin zuten erasotzaileek spear-phishing kanpainak banatzeko erabili zutela ahultasun hori. Erasoaren hasierako fasea 2021eko abenduaren 14an izan zen, Outlook.com-eko 74 helbide elektroniko bakar erabiliz, guztiak erasotzaileek sortuak. Bidalketa-denboren ereduak iradokitzen du eskuz sor zezaketela bidalitako mezu elektroniko bakoitzaren edukia.

Egindako ikerketaren arabera, ez zuten ingeniaritza sozialeko teknika konplexu bat erabili, baizik eta erabiltzailearen eta jasotako posta elektronikoaren arteko interakzioan zentratu ziren. Aztertutako mezu guztiek irudi bat zuten erantsita, eta gai generikoak zituen gai bat erakusten zuten, hala nola gonbidapenak, hegazkin txartelak itzultzea edo ohartarazpenak. Irudietako bakoitzak esteka bat zuen erantsita, bitxia bada ere, esteka bakoitza bakarra zen helburu baterako, eta horrek, ziurrenik, erasotzaileei balio izan zien phishing mezuak zein helbide elektronikok irekitzen zituzten egiaztatzeko. Hona hemen urruneko irudiei zuzendutako URL helbideen adibideak:

- *hxxp://fireclaws.spiritfield[.]ga/[fitxategiaren izena].jpeg?[Zenbakia]*
- *hxxp://feralrage.spiritfield[.]ga/[fitxategiaren izena].jpeg?[Zenbakia]*
- *hxxp://oaksage.spiritfield[.]ga/[fitxategiaren izena].jpeg?[Zenbakia]*
- *hxxp://claygolem.spiritfield[.]ga/[fitxategiaren izena].jpeg?[Zenbakia]*

URL bakoitzaren amaierako zenbakiak biktima espezifikoki identifikatzeko balio du. Aurkitu zen azpidomeinuak ere bakarrak zirela posta elektroniko bakoitzarentzat, baina ez dakigu zergatik aukeratu ziren.

Hala ere, eduki guztia ez zen pertsonalizatu edo eskuz egin helburuak bereizteko. Ondorengo spear-phishing olatuak, neurri handi batean, generikoak izan ziren, eta, gehienak, Gabonetako denboraldiarekin lotuak, bereziki, zenbait hegazkin konpainia edo Amazon bezalako multinazionalak ordezkatu nahi zituzten. Bigarren fase honetan erabilitako URLek aurrekoen antzeko patroia jarraitu zuten, baina azpidomeinu sendoarekin. Hona hemen adibide bat:

- *hxxps://update.secretstep[.]tk/[fitxategiaren izena].jpeg?u=[zenbakia]&t=[erakundea]*

Kasu horretan, URLaren amaierak helburu erakundea adierazten du. Iruzurrezko estekara sartzean, erasotzailea erabiltzailea helburuko erakundearen Zimbra sistemaren baliabide batera bideratzen saiatuko da, URL formatu espezifiko bat erabiliz. Puntu horretara iritsita, biktimak Zimbrako saioa hasita jarraitzen badu, ahultasunaren ustiapen arrakastatsua gertatzen da, eta JavaScript kodea kargatzeko aukera ematen du hasitako Zimbrako saio baten testuinguruan. Ahultasun horretarako adabakirik ez dagoenez, Volexityk ez du gaur egun ustiaketa arrakastatsu baterako behar den URL patroia erakutsi. Hala ere, erabilitako kodearen kopia iragazi bat kontsulta daiteke esteka honetan.

Erasotzailearen kodearen funtzionaltasuna sinplea da. Lehenik eta behin, kodeak mezu elektroniko bakoitza ikuskatzen du erabiltzailearen sarrera-erretiluan, bai eta bidalitako karpetak ere. Ondoren, aurkitutako mezu elektroniko bakoitzeko, kodeak mezu elektronikoaren gorputza eta erantsitako fitxategiak dei zehaztua itzultzeko helbidera (mail.bruising-intellect[.]ml) bidaltzen ditu, HTTP POST eskaeren bidez.

Eraso horren ondorio nagusia da erasotzaileak iruzurrezko estekara sartzea lortzen badu eta nabigatzailearen leihoa irekita edukitzen badu denbora-tarte batez, postontziaren eduki guztia eskuratu ahal izango duela. Kontuan hartu behar da posta-lapurreta errazteko erabiltzen den JavaScript kodea biktimak erabiltzen duen Zimbraren bertsioaren arabera pertsonalizatu behar dela, erasotzaileak CSRF tokena duen orri bat eskatu behar baitu posta-datuak lapurtzeko behar diren eskaerak egiteko.

Bezeroaren aurkako erasoetan erabilitako azpiegituraren arabera, Volexityk erabaki zuen identifikatutako azpiegitura guztiak Freenom domeinuak erabili zituela AS399269 unitatean, BitLaunch-en (BLNWX). Horiek zerbitzari pribatu birtualak dirudite, eta ziur aski bitlaunch.io zerbitzuaren bidez erosi ziren. Zerbitzu horrek azpiegitura erosteko aukera ematen du kriptomonedak erabiliz. Halaber, ikusi zen identifikatutako IP helbide guztiek Apache 2.4.6 exekutatzen zutela Centos-en PHP 5.4.16 erabiliz. TLS ziurtagiriak Zero SSLren bidez erosi ziren.

Esleipenari dagokionez, Volexityk identifikatutako azpiegituretako bat ere ez dator guztiz bat aurrez identifikatutako mehatxu-taldeek erabilitako azpiegiturarekin. Hala ere, antolaketa eta helburuak aztertu ondoren, badirudi APTko aktore txinatar batek egin dituela erasoak, TEMP_Heretic izenekoa.

3. ARINTZEA / KONPONBIDEA

Ohiko moduan, ahultasun hori eta beste batzuk saihesteko, BCSCk gomendatzen du sistemak eta aplikazioak eguneratuta izatea eskuragarri dagoen azken bertsioan.

Ahultasunak Zimbra 8.8.15 bertsioari eta aurrekoei eragiten die. Konpainiak oraindik adabaki ofizialik ez duenez, Zimbraren softwarea bertsio berrienera (9.0.0 bertsioa) eguneratzea gomendatzen zaie erabiltzaileei.

Halaber, Zimbraren erabiltzaile guztiek beren datu historikoak aztertu behar dituzte erreferentzia eta sarbide susmagarriak bilatzeko. Erregistro horien kokaleku lehenetsia hemen aurki daiteke: */opt/zimbra/log/access*.log.*

Horrez gain, erabiltzaileei gomendatzen zaie posta elektronikoaren lotura-atean eta sare-mailan IOC hauek blokeatzea:

Valor	Tipo Entidad	Descripción
www[.]newsonline[.]gq	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
mx[.]newsonline[.]gq	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
www[.]spiritx[.]ga	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
soporte[.]newsonline[.]gq	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
www[.]thunderchannel[.]tk	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
shadownight[.]playquicksand[.]tk	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
www[.]windsoft[.]cf	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
tigerstrike[.]iceywindflow[.]ml	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
shadowmaster[.]iceywindflow[.]ml	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
www[.]iceywindflow[.]gq	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
cargadoboltsentry[.]spiritfield[.]tk	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
noticiassonline[.]gq	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura

espíritux[.]ga	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
pasosecreto[.]tk	Host izena	Zimbra 0-Day programarekin batera erabilitako azpiegitura. Erabiltzaileak Zimbrako URL maltzurrera bideratzeko erabiltzen den hasierako domeinua.
Spiritfield[.]ga	Host izena	Zimbra 0-Day programarekin batera erabilitako azpiegitura. Ezagutza-mezu elektronikoetan erabiltzen da, helbideak benetakoak ziren baliozkotzeko, karga erreala geroago bidali aurretik.
www[.]noticias-voz[.]ml	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
www[.]encontrarlaverdad[.]ml	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
noticias-online[.]ml	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
iceywindflow[.]gq	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
playquicksand[.]tk	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
windsoft[.]cf	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
encontrarlaverdad[.]ml	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
iceywindflow[.]ml	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
noticias-voz[.]ml	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
moretones-intelecto[.]ml	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
canaltrueno[.]tk	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
Spiritfield[.]ml	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
iceywindflow[.]cf	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura

truenocanal[.]cf	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
Spiritfield[.]tk	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
actualizar[.]secretstep[.]tk	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
mail[.]bruising-intelecto[.]ml	Host izena	Zimbra 0-Day programarekin batera erabilitako azpiegitura. JS gaiztoak erabiltzaileen posta lapurtzen zuen eta C2 zen JS maltzur horrentzat.
www[.]noticias-online[.]ml	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
www[.]thunderchannel[.]cf	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
www[.]spiritfield[.]ga	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
winderosion[.]spiritfield[.]ml	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
flameshock[.]spiritfield[.]tk	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
windsource[.]thunderchannel[.]cf	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
yahoo-movie[.]spiritx[.]ga	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
windsource[.]thunderchannel[.]tk	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
opticaleel[.]iceywindflow[.]cf	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
shadownight[.]spiritfield[.]ga	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
206[.]166[.]251[.]141	IP helbidea	Zimbraren ustiapenarekin lotutako jabari ezagunerako ebazpena
206[.]166[.]251[.]166	IP helbidea	Zimbraren ustiapenarekin lotutako jabari ezagunerako ebazpena
108[.]160[.]133[.]32	IP helbidea	Lotutako C2 zerbitzariaren susmoa
172[.]86[.]75[.]158	IP helbidea	Zimbraren ustiapenarekin lotutako jabari ezagunerako ebazpena

www[.]yahoo-corporation[.]ml	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
amazon-check[.]gq	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
amazon-equipo[.]tk	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
yahoo-corporation[.]ml	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
playquicksand[.]gq	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
yahoo-corporation[.]tk	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
playquicksand[.]cf	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
Spiritfield[.]cf	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
amazon-check[.]ga	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
amazon-check[.]cf	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
amazon-check[.]tk	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
playquicksand[.]ml	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
www[.]playquicksand[.]cf	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
www[.]amazon-check[.]ga	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura
www[.]playquicksand[.]gq	Host izena	Ziurrenik Zimbra 0-Day programarekin batera erabiliko den azpiegitura

4. ERREFERENTZIA OSAGARRIAK

- Operation EmailThief: Active Exploitation of Zero-day XSS Vulnerability in Zimbra.
- Hotfix Available 5 Feb for Zero-day Exploit Vulnerability in Zimbra 8.8.15.
- Operation EmailThief: Zero-day XSS vulnerability in Zimbra email platform revealed.
- threat-intel/2022/2022-02-03Operation emailThief/attachments/zimbra_mailtheft_code.js.beautified.
- Zimbra: A synacor product.
- threat-intel/2022/2022-02-03 Operation EmailThief/indicators/iocs.csv.
- ¿Qué es un token CSRF? ¿Cuál es su importancia y cómo funciona?
- Freenom - Un nombre para todo el mundo.
- BitLaunch.
- ZeroSSL.

Gertakarien jakinarazpena

Zibersegurtasun gertakariren bat aurkitu baduzu jakinaraz iezaguzu, horrela beharrezkoak diren neurriak hartuko ditugu zabal ez dadin.

900 104 891

arazoak@bcsc.eus

Zibersegurtasun katalogoa

Zure zibersegurtasunarekin edo zure enpresarenarekin laguntza behar duzu?