



Zerobot malwarea ezartzeko ustiatutako ahultasunak

TLP: CLEAR

www.ciberseguridad.eus



AURKIBIDEA

BCSC-ri buruz	3
1. Laburpen exekutiboa	¡Error! Marcador no definido.
2. Azterketa teknikoa	¡Error! Marcador no definido.
3. Arintza / Konponbidea	¡Error! Marcador no definido.
4. Erreferentzia osagarriak	¡Error! Marcador no definido.

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 konsideratu 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 elektronikoien 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

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

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:



1. Laburpen exekutiboa

Microsoften ikerketa taldeak ([MSTIC](#)) Zeroboten eguneratzeari buruzko ikerketa bat [argitaratu](#) du, malware-as-a-service gisa eskainitako bot-sare bat, Go-n oinarritua eta web eta IoT aplikazioei eragiten dieten hainbat ahultasun baliatzen dituena.

Zeroboten erabilitako azken bertsioa aztertu ondoren, ikertzaileek beren ahultasun zerrendari egindako espoilten batura detektatzea lortu dute. Guztira, zazpi akats nabarmen identifikatu ahal izan dituzte, larritasun handia edo kritikoa dutelako. Horien artean, [Apache HTTP Server](#) eta [Apache Spark](#) sistemei eragiten dieten 2 ahultasun daude.

Beren kanpainetan ustiatiu beharreko urrakortasun berriak eranstearen helburua da mehatxu eragileek firewall gailuen, router-en eta gainerako sistema kalteberen infekzioa areagotzeko asmoa dutela, banatutako zerbitzua ukatzeko boten sarean (DDoS) gehitzeko.

Sistema kalteberen fabrikatzaileetako batzuek dagoeneko argitaratu dituzte dagozkien adabakiak, eta, horrela, akats nabarmenak zuzendu dituzte. Beraz, ahultasun horiek eta beste batzuk prebenitzeko, BCSCK sistema eta aplikazioak eskuragarri dagoen azken bertsioan eguneratuta izatea gomendatzen du, dagozkion adabakiak argitaratu bezain laster.

2. Azterketa teknikoa

Zeroboten 1.1 bertsioak barne hartzen dituen ahultasunak, horietako bat izan ezik, kritikotasun handiarekin kalifikatu ditu [NISTk](#).

Lehenik eta behin, [CVE-2017-17105](#) eskalan identifikatutako ahultasuna zehazten da. Larritasun hori kritikoa da, eta 9.8ko puntuazioa ematen zaio [CVSSv3](#) eskalaren arabera. Akats hori Silas Cutler ikertzaileak jakinarazi zuen hasiera batean, eta, horri esker, autentifikatu gabeko urruneko erasotzaile batek kode arbitrarioa injektatu dezake [CGI scripten](#) bidez. Errore horrek Zivif PR115-204-P-RS web kameren bertsio desberdinei eragiten die. Nabarmendu behar da publikoki kontzeptu proba bat (PoC) erabilgarri dagoela [deskribatutako](#) akatsa ustiatzeko.

Jarraian, [CVE-2019-10655an](#) katalogatutako ahultasuna nabarmenzen da, eta larritasun kritikoa du, 9.8ko puntuazioa baitu [CVSSv3](#) eskalaren aldean. Ahultasun horrek aukera ematen dio autentifikatu gabeko urruneko erasotzaile bati xede sisteman kode arbitrarioa exekutatzeko shell [metakarakterren](#) bidez, eta, horrela, bufer gainezkatzea eragiten du. Mehatxu eragile batek datu egitura maltzur bat gainidatz dezake, sistemaren autentifikazioa saihestuz. Ahultasun horrek Grandstream GAC2500, GXP2200, GVC3202 eta GXV3275 gailuei eragiten die, eta urrunetik edo Cross-Site Request Forgery ([CSRF](#)) bidez ustiatu daiteke. Era berean, sarbide [publikoko](#) Metasploiteko modulu bat identifikatu da, kontzeptuzko proba bat duena (PoC), deskribatutako akatsa ustiatzeko.

Hirugarren ahultasun nabarmena [CVE-2020-25223an](#) identifikatuta dago, eta zorroztasun kritikoa du, 9.8ko puntuazioa baitu [CVSSv3](#) eskalaren aldean. Ezagutzen da urruneko erasotzaile batek urruneko kode arbitrarioa exekutatzeko aukera duela Sophos SG UTMren bertsio desberdinan. Horrez gain, kontzeptu-proba bat (PoC) duen Metasploiteko modulu bat [argitaratu](#) dela antzeman da, deskribatutako akatsa ustiatzeko.

Detektatutako laugarren errorea [CVE-2021-42013an](#) erregistratuta dago, eta zorroztasun kritikoa du, 9.8ko puntuazioa baitu [CVSSv3](#) eskalaren arabera. Autentifikatu gabeko urruneko erasotzaile baten ahultasuna, eragindako zerbitzariari bereziki diseinatutako HTTP eskaera bat bidaltzea eta sistema eragilearen komando arbitrarioak exekutatzea xede-sisteman. Erroreak Apache zerbitzarien bertsio desberdinak ukitzen ditu, eta hainbat kontzeptu-proba ditu (PoC), esteka hauen bidez eskura daitezkeenak:

- Apache HTTP Server 2.4.50 Path Traversal / Code Execution.
- Apache 2.4.49 / 2.4.50 Traversal / Remote Code Execution.
- Apache HTTP Server 2.4.50 Remote Code Execution.
- Apache 2.4.50 Remote Code Execution.

Jarraian, [CVE-2022-31137an](#) erregistratutako ahultasuna aurkituko dugu. Zorroztasun kritikoa du, 9.8ko puntuazioa bai [CVSSv3](#) eskalan. Ahultasuna subprocess_execute () funtziaren bidez fitxategi/app/options.py-ra igarotako sarrera-balidazio desegokiaren ondorioz dago. Autentifikatu gabeko urruneko erasotzaile batek HTTP eskaera bat pasa dezake, bereziki diseinatua, eta sistema eragilearen komando arbitrarioak exekutatu xede-sisteman. Nabamentzekoa da akats horrek Roxi-WI web interfazeari eragiten diola, eta jendaurrean [kontsulta](#) daitekeen exploit bat duela.

Seigarren ahultasunak, [CVE-2022-33891aren](#) azpian identifikatuak, zorroztasun handia du, 8.8ko puntuazioarekin, [CVSSv3](#) eskalaren arabera. Urrakortasuna [Apache Spark](#)-en erabiltzaile-interfazearen barruan [ACL](#) funtziaren sarrera desegokia baliozkotzearen ondorioz dago. Urruneko erabiltzaile batek bereziki diseinatutako URL bat eska dezake, eta xede-sisteman sistema eragilearen komando arbitrarioak exekutatu. Ahultasun horren ustiapen arrakastatsua sistema kalteberaren konpromiso osoan gerta daiteke, baina [spark.acls.enable](#) aukera aktibatuta egotea eskatzen du. Nabamentzekoa da Metasploiteko modulu bat modu [publikoan](#) detektatu dela, deskribatutako ahultasunari buruzko kontzeptu-proba bat (PoC) zehazten duena.

Azkenik, Gjoko Krstic ikertzaileak jakinarazitako eta [ZLS-2022-5717](#) katalogatutako urrakortasunari zorroztasun kritikoz eman zaio puntuazioa. Jakin badakigu akats horrek aukera ematen diola autentifikatu gabeko urruneko erasotzaile bati root-pribilegioak dituen kode arbitrarioa exekutatzeko. Argitaratutako oharrean, MiniDVBLinux-i eragiten dion errorea aprobetxatzeko xehetasunak ematen dituen kontzeptu-proba batera (PoC) bideratzen duen [esteka](#) bat dago.

Hauek dira aurreko ahultasunek eragindako produktuak:

- Zivif PR115-204-P-RS 2.3.4.2103 – 4.7.4.2121 bertsioak.
- Granstream GAC2500 1.0.3.35 bertsioa.
- Granstream GXP2200 1.0.3.51 bertsioa.
- Granstream GXV3275 1.0.3.219 Betaren aurreko bertsioak.
- Granstream GXV3240 1.0.3.219 Betaren aurreko bertsioak.

- Sophos SG UTM v9.705 MR5, v9.607 MR7 eta v9.511 MR11ren aurreko bertsioak.
- Apache HTTP Server 2.4.50 bertsioa.
- Roxi-WI 6.1.1.0ren aurreko bertsioak.
- Apache Spark 3.03 bertsioak eta aurrekoak, 3.1.1 – 3.1.2 eta 3.2.0 – 3.2.1.
- MiniDVBLinux 5.4 bertsioa eta aurrekoak.

3. Arintzea / Konponbidea

Ohikoa denez, urrakortasun hori eta beste batzuk prebenitzeko, BCSCk sistema eta aplikazioak eskuragarri dagoen azken bertsioan eguneratuta izatea gomendatzen du, dagozkion adabakiak argitaratu bezain laster.

Garrantzitsua da neurriak azkar hartza, implementazio-arazo horiek arintzeko. Horregatik, ahultasunen larritasuna dela eta, fabrikatzaileek proposatutako irtenbide ofizialak aplikatzea gomendatzen da, esteka hauetan eskuragarri daudenak:

- [Grandstream GAC2500 1.0.3.45 bertsioa.](#)
- [Grandstream GVC3202 1.0.3.69 bertsioa.](#)
- [Grandstream GXV3275 1.0.3.227 bertsioa.](#)
- [Grandstream GXV3240 1.0.3.227 bertsioa.](#)
- [Apache HTTP Server 2.4.54 bertsioa.](#)
- [Roxi-WI 6.1.1.0 bertsioa.](#)
- [Apache Spark 3.3.1 bertsioa.](#)
- [MiniDVBLinux 5.5 bertsioa.](#)

Nabarmentzekoa da gaur egun ez dagoela [CVE-2017-17105erako](#) irtenbide ofizialik. [CVE-2019-10655ari](#) dagokionez, [hornitzaireak](#) ez du akats hori konponduko duen arintzerik argitaratu Granstream GXP2200en.

Azkenik, MiniDVBLinuxen 5.5 bertsioa ez da egonkorra, baina instalatzea gomendatzen da, [ZLS-2022-5717](#) azpian erregistratutako ahultasun kritikoa arintzen baitu.

4. Erreferentzia osagarriak

- MSTIC.
- Microsoft research uncovers new Zerobot capabilities.
- Apache HTTP Server.
- Apache Spark.
- NIST.
- NVD: CVE-2017-17105.
- NVD: CVE-2019-10655.
- NVD: CVE-2020-25223.
- NVD: CVE-2021-42013.
- NVD: CVE-2022-31137.
- NVD: CVE-2022-33891.
- ZLS-2022-5717.
- First organization.
- Contenido dinámico con CGI.
- Zivif PR115-204-P-RS 2.3.4.2103 Bypass / Command Injection / Hardcoded Password.
- Comandos en Linux: metacaracteres, entrecomillado y caracteres especiales.
- ¿En qué consiste la vulnerabilidad Cross Site Request Forgery (CSRF)?
- Grandstream GXV3175 Unauthenticated Command Execution.
- Sophos UTM WebAdmin SID Command Injection.
- Apache HTTP Server 2.4.50 Path Traversal / Code Execution.
- Apache 2.4.49 / 2.4.50 Traversal / Remote Code Execution.
- Apache HTTP Server 2.4.50 Remote Code Execution.
- Apache 2.4.50 Remote Code Execution.
- Roxy-WI Remote Command Execution.
- Lista de control de acceso (ACL) en la red.
- ACL Configuration for Spark.
- Apache Spark Unauthenticated Command Injection.
- PoC: ZLS-2022-5717.

- Grandstream GAC2500 versión 1.0.3.45.
- Grandstream GVC3202 versión 1.0.3.69.
- Grandstream GXV3275 versión 1.0.3.227.
- Grandstream GXV3240 versión 1.0.3.227.
- Apache HTTP Server versión 2.4.54.
- Roxi-WI versión 6.1.1.0.
- Apache Spark versión 3.3.1.
- MiniDVBLinux versión 5.5.
- Grandstream Important Firmware News.

 Basque
CyberSecurity
Centre