KCodes NetUSB ahultasuna

BCSC-AHULTASUNA-KCODES-NETUSB

TLP:WHITE

www.basquecybersecurity.eus

2022ko Urtarrila

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:

1. LABURPEN EXEKUTIBOA

SentinelLabs-eko segurtasun-ikertzaileek ahultasun kritikoa aurkitu dute KCodes NetUSB kernel moduluan. Modulu hau mundu osoko sare-gailuen hornitzaile askok erabiltzen dute, eta, beraz, akats horrek eragina izan dezake azken erabiltzaileen milioika routerretan. Ahultasun hori CVE-2021-45608 zenbakiarekin erregistratu da, eta erasotzaileek urrunetik egin dezakete kodea kernelean. NetUSB modulu kalteberak erabiltzen dituzten bideratzaileen hornitzaileak hauek dira: Netgear, TP-Link, Tenda, EDiMAX, Dlink eta Western Digitala.

NetUSB KCodek garatutako produktu bat da, routerraren USB ataken bidez inprimagailuak, disko gogorrak edo pendriveak konektatu ahal izateko diseinatuta dagoena. Abiadura mugatuagoa bada ere, sareko edozein puntutatik gailuetara sartzeko modu erosoa da. Adibidez, erabiltzaile batek inprimagailu batekin elkarreragin dezake, USB bidez ordenagailura zuzenean konektatuta balego bezala. Horretarako, kernelaren modulu honen bidez routerrarekin komunikatzen den gailuan kontrolatzaile bat behar da.

SentinelLabsetik, uko egin diote kontzeptuaren froga-kode bat (POC) argitaratzeari, beste hornitzaile batzuk oraindik eguneratzeak bidaltzeko prozesuan daudelako. Hala ere, zibersegurtasuneko enpresak ohartarazi zuen exploit bat sor zitekeela, nahiz eta teknikoki konplexua izan; beraz, nahitaezkoa da erabiltzaileek zuzenketak aplikatzea, balizko edozein arrisku arintzeko. Bestalde, adierazi dute gaur egun ez dela aurkitu ahultasuna ustiatu izanaren ebidentziarik.

Ahultasun hori zabaltzeko prozesua irailaren 9an hasi zen, eta adabakia urriaren 4an bidali zitzaien hornitzaileei. Gailu kalteberen ahultasunari heltzen dioten firmware-en eguneratzeak joan den abenduan hasi ziren ezartzen.

2. AZTERKETA TEKNIKOA

Ahultasunak KCodes NetUSB kernelaren moduluari eragiten dio, eta horrek USB ataka bat duten router askori eragin liezaieke. USB ataka horien errendimendua ahalik eta gehien aprobetxatzeko, fabrikatzaileek NetUSB izeneko kernel modulu bat dute, KCodesek garatua. Konektibitate modulu honek aukera ematen die sareko gailuei urrutitik sartzeko, routerrarekin konektatuta dauden USB gailu guztiekin elkarreragiteko.

Zoritxarrez, modulu honen kodean ahultasun kritikoa aurkitu da, kernelaren beraren memoria esleipenen tamainaren balioa baliozkotzea eragozten duena, eta horrek osoen gainezkatzea eragiten du. Zehazki, SoftwareBus_fillBuf funtzioak urruneko kodea sartzeko aukera ematen dio erasotzaile bati, gailu kaltebera konektatuta dagoen sarean jarduera kaltegarriak egiteko.

Ahultasun hori ustiatzea konplexua da, bete behar dituen muga batzuk direla-eta; esate baterako, pakete osoak gainezka egiteko bidalitako paketearen tamaina zehatza 32 bytetik beherakoa izan behar da, kmalloc-32an sar dadin. Hala ere, NetUSB modulu kalteberak hamasei segundoko itxaronaldia du eskaera bat jasotzeko, eta horrek malgutasun handiagoa ahalbidetzen du gailu bat ustiatzean.

Murrizketa horiek ahultasun horretarako exploit bat sortzea zailtzen badute ere, ez da guztiz ezinezkoa; horregatik, Wi-Fi routerrak dituzten erabiltzaileei beren gailuekin bateragarriak diren firmware eguneratzeak bilatzea gomendatzen zaie.

SentinelOnek ez du kontzeptu frogarik (POC) argitaratu, beste hornitzaile batzuk oraindik eguneratzeak bidaltzeko prozesuan daudelako. Baina zibersegurtasuneko enpresak ohartarazi zuen exploit bat sor zitekeela, nahiz eta teknikoki konplexua izan, eta, beraz, nahitaezkoa da erabiltzaileek zuzenketak aplikatzea edozein arrisku potentzial arintzeko.

3. ARINTZEA / KONPONBIDEA

Ohikoa denez, ahultasun hori eta beste batzuk prebenitzeko, BCSCtik gomendatzen da sistemak eta aplikazioak beti eguneratuta izatea eskuragarri dagoen azken bertsioan, adabakiak argitaratu bezain laster.

Ahultasun hori hainbat bideratzailerentzako lizentzia duten hirugarrenen osagai baten barruan dagoenez, zure routerraren firmwarea eguneratzea gomendatzen da, eguneratzerik badago. Garrantzitsua da egiaztatzea zure routerra ez dela eredu bat bizitza baliagarriaren amaieran, oso zaila baita ahultasun horretarako eguneraketa bat jasotzea.

Zehazki, ukitutako fabrikatzaileen artean honako hauek nabarmentzen dira: NETGEAR, TP-Link, Tenda, EDiMAX, eta Dlink, Western Digitalaz gain, sareko disko gogorrek ere erabiltzen baitituzte sareko modulu horiek. Ikertzaileek ez dituzte kaltetutako ereduak zehaztu, baina zure gailuak USB atakak baditu, litekeena da erasanda egotea.

Ahultasun hori zabaltzeko prozesua irailaren 9an hasi zen, eta adabakia urriaren 4an bidali zitzaien hornitzaileei. Gailu kalteberen ahultasunari heltzen dioten firmware-en eguneratzeak joan den abenduan hasi ziren ezartzen.

Fabrikatzaile guztiek ez dute jakinarazi ahultasunei adabakiak jarri dizkietela, eta, beraz, denbora gehiago beharko dute horretarako. Gaur egun ez da aurkitu erasotzaileek ahultasuna ustiatu duten ebidentziarik.

4. ERREFERENTZIA OSAGARRIAK

- CVE-2021-45608 | Falla de NetUSB RCE en millones de enrutadores de usuarios finales
- CVE-2021-45608 Detail
- SentinelLabs
- KCodes NetUSB bug exposes millions of routers to RCE attacks.
- SOHO routers impacted by bug in USB-over-network
- KCodes NetUSB kernel remote code execution flaw impacts millions of devices

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?