Ahultasuna Windows-en (CVE-2021-41379)

BCSC-AHULTASUNA-WINDOWS-CVE-2021-41379

TLP:WHITE

www.basquecybersecurity.eus

2021eko azaroa

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.

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

Joan den azaroaren 9an, Microsoft-ek eguneratzeak argitaratu zituen 55 ahultasun konpontzeko, eta horietatik 49k kritikotasun handia zuten. Ahultasun horietako batek, CVE-2021-41379 izenekoak, sarrera mugatua zuten erabiltzaileei sistemaren barruan pribilegioak eskalatzeko aukera ematen zien. Nahiz eta teorian eguneratzearekin konpondu behar izan, ez da hala izan.

Abdelhamid Nacerik, ahultasunaren berri eman zuen ikertzaileak, Microsoftek proposatutako irtenbidea saihestea lortu du, eta, era berean, administrazio-baimenak lortu ditu. Ahultasun horrek Windowsen bertsio guztiei eragiten die, Windows 10, Windows 11 eta Windows Server 2022 barne. Gainera, Nacerik exploit bat argitaratu du ahultasun hori ustiatzeko. Lotura honetan dago:

- GitHub: InstallerFileTakeOver.

Ahultasun hori ez zaio konpainiari jakinarazi ohiko bideak erabiliz; izan ere, Naceriren arabera, akats horien ondorioz Microsoftek eskaintzen dituen sari ekonomikoak gutxitzen joan dira denboran zehar.

Microsoftetik oraindik ez da ofizialki argitaratu zikloz kanpoko eguneraketarik ahultasun hori konpontzeko. Hala ere, abenduko eguneratzeen hurrengo argitalpenean beste irtenbide bat aurkeztea espero da.

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.

2. AZTERKETA TEKNIKOA

Ahultasun hori, pribilegioak eskalatzeko aukera ematen duena, joan den azaroaren 9an argitaratu zen, hileko eguneratzeen argitalpenaren zati gisa. Hona hemen konpainiak hilabete hasierako txostenean argitaratutako xehetasun teknikoak:

- CVE-2021-41379: Aplikazioak ez ditu behar bezala ezartzen Windows-eko instalatzailearen segurtasun murrizketak, eta, beraz, segurtasun murriztapenak alde batera uzten ditu, eta oinarrizko baimenak dituzten tokiko erabiltzaileei sisteman pribilegioak mailakatzeko aukera ematen die.

Hasieran uste zen konpainiak proposatutako konponbidearekin ahultasuna eten egiten zela. Hala ere, Abdelhamid Nacerik, akats hori aurkitu eta Microsoft-i jakinarazi zion ikertzaileak, ikusi du DACL sarbide diskrezionaleko control zerrenda gainidatzi daitekeela. Microsoft Edge-ren jasotze zerbitzuaren zerrenda hori bere buruari kopiatzen zaio zerbitzuaren kokapenean, eta pribilegio handiak lortzeko exekutatzen da.

Abdelhamid Nacerik berak, haren arabera animatuta, enpresak aurkikuntza horiengatik ematen duen sari eskasagatik, lehergailu bat argitaratu du ahultasun hori ustiatzeko, eta adierazi du ezen, nahiz eta talde politikak eratu daitezkeen pribilegio gutxiko erabiltzaileek MSI instalatzeko eragiketak egin ez ditzaten, lehergailu hori politika hori alde batera utzi eta dena dela funtzionatzen duela.

- GitHub: InstallerFileTakeOver.

Bleepingcomputer-eko taldeak kontzeptu proba bat partekatu du, eta, proba horretan, exploit horren funtzionamendua ikus daiteke:

- PoC: New windows zero-day local privilege elevation vulnerability.

Ahultasunak Windowsen bertsio bateragarri guztiei eragiten die: Windows 10, Windows 11 eta Windows Server 2022 barne.

3. ARINTZEA / KONPONBIDEA

Microsoftetik oraindik ez da argitaratu ahultasun hori saihesteko konponbiderik. Hala ere, abenduko ahultasunak argitaratuta konpontzea espero da.

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.

4. ERREFERENTZIA OSAGARRIAK

- New Windows zero-day with public exploit lets you become an admin.
- Windows Installer Elevation of Privilege Vulnerability: CVE-2021-41379.
- Privilege escalation in Microsoft Windows Installer.
- PoC: New windows zero-day local privilege elevation vulnerability.
- GitHub: InstallerFileTakeOver.
- DACL y ACE.
- NIST: CVE-2021-41379.
- Cuenta twitter: Abdelhamid Naceri.

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?