Basque CyberSecurity Centre

Ahultasun kritikoaren ustiapena VMware Workspace One Access-en (CVE-2022-22954)

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

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:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Laburpen exekutiboa

VMware Workspace One Access, aplikazioen banaketa eta kudeaketa errazten eta babesten duen lan-eremu digitala, gogortasun kritikoko ahultasuna du, eta modu aktiboan ustiatzen ari da.

Akats hori CVE-2022-22954-ren arabera katalogatuta dago, eta urruneko erasotzaile bati arbitraje-kodea exekutatzeko aukera ematen dio. Ikertzaileek ikusi dute akats horretaz berriro baliatzen ari direla programa maltzurrak ezartzeko, *RAR1Rasom* tresnaz gain, konprometitutako sistemetan pasahitzez babestutako fitxategiak enkriptatzeko gai dena. Era berean, erasotzaileek gailu urratuen baliabideak erabiltzen dituzte *GuardMiner* programaren bidez kriptomonedak minatzeko.

Aurrekoaz gainera, akats nabarmena ustiatu dela ikusi da zerbitzua ukatzeko (DDoS) eraso banatuak egiteko, *Mirai* izeneko botnetaren bidez.

Ahultasun hori apirilaren 6an partxekatu zen, eta une horretan argitaratutako exploit-ak aurkitu ziren. APT35en sistema ahuletan atzeko ateak jartzeko egindako jarduera maltzurra nabarmendu zen.

Lehenago aipatu bezala, VMware-k akats hori zuzentzen duen partxe ofiziala argitaratu zuen, eta, beraz, ahultasun hori eta beste batzuk prebenitzeko, BCSCk gomendatzen du sistemak eta aplikazioak eguneraturik izatea eskuragarri dagoen azken bertsioan, dagozkion partxeak argitaratu bezain laster.

2. Azterketa teknikoa

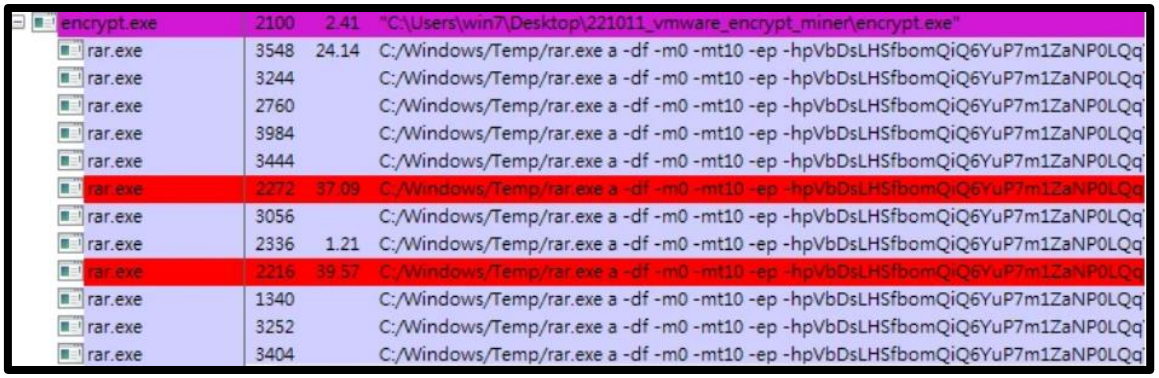
Ahultasun nabarmenak VMware Workspace One Access-i eragiten dio eta CVE-2022-22954-ren bidez identifikatuta dago, urruneko erasotzaile bati helmugako sisteman arbitraje-kodea exekutatzeko aukera ematen dio. Sarrera baliozkotze desegoki batek eragin du akatsa. Urruneko erasotzaile batek bereziki diseinatutako HTTP eskaera bidal dezake eta zerbitzariaren aldeko txantiloi-injekzio bat egin.

Akats hori azaltzen duten kanpaina berrietan, zenbait etiologia maltzur nabarmentzen dira, Cloudflaretik artxibo hauek deskargatzen hasteko bektore gisa erabiltzen dituztenak:

- *phpupdate.exe*: *GuardMiner*.
- *config.json*: *GuardMiner-erako* konfigurazio-fitxategia.
- *networkmanager.exe*: malwarea eskaneatu eta zabaltzeko exekutagarria.
- *phpguard.exe*: bere funtzioa *GuardMiner-en* funtzionamendua mantentzea da.
- *clean.bat*: meatzaritzari lotutako beste programa batzuk kentzea.
- *cifrar.exe*: *RAR1Rasom* tresna.

Lehenik eta behin, *GuardMiner* software baten inplementazioa aztertuko dugu. *Monero* minatzeko konprometitutako sistemaren baliabideak erabiltzen ditu software horrek. Programa honek beste hosts batzuetara hedatzeko gaitasuna du, besteak beste, Apache Struts, Atlassian Confluenceeta Spring Cloud Gatewayn dauden beste ahultasun batzuk aprobetxatuz. Aurrekoaz gain, programa hau troiatar oso gisa kalifikatu da, eta PowerShell komandoak exekutatu eta sistemetan iraunkortasuna ezar dezake programatutako ataza berriak gehitzean.

RAR1Rasom erasoei dagokienez, esan behar da ransomware-tresna bat dela, eta WinRARek erabiltzen duela biktimen gailuetako fitxategiak konprimitzeko, eta, ondoren, erabiltzaileek ezagutzen ez duten pasahitz baten bidez blokeatu egiten dituela. Hona hemen tresna horrek datuak zifratzeko erabiltzen dituen prozesuen lagin bat:



encrypt.exe	2100	2.41	"C:\Users\win7\Desktop\221011_vmware_encrypt_miner\encrypt.exe"
rar.exe	3548	24.14	C:/Windows/Temp/rar.exe a -df -m0 -mt10 -ep -hpVbDsLHSfbomQiQ6YuP7m1ZaNP0LQq
rar.exe	3244		C:/Windows/Temp/rar.exe a -df -m0 -mt10 -ep -hpVbDsLHSfbomQiQ6YuP7m1ZaNP0LQq
rar.exe	2760		C:/Windows/Temp/rar.exe a -df -m0 -mt10 -ep -hpVbDsLHSfbomQiQ6YuP7m1ZaNP0LQq
rar.exe	3984		C:/Windows/Temp/rar.exe a -df -m0 -mt10 -ep -hpVbDsLHSfbomQiQ6YuP7m1ZaNP0LQq
rar.exe	3444		C:/Windows/Temp/rar.exe a -df -m0 -mt10 -ep -hpVbDsLHSfbomQiQ6YuP7m1ZaNP0LQq
rar.exe	2272	37.09	C:/Windows/Temp/rar.exe a -df -m0 -mt10 -ep -hpVbDsLHSfbomQiQ6YuP7m1ZaNP0LQq
rar.exe	3056		C:/Windows/Temp/rar.exe a -df -m0 -mt10 -ep -hpVbDsLHSfbomQiQ6YuP7m1ZaNP0LQq
rar.exe	2336	1.21	C:/Windows/Temp/rar.exe a -df -m0 -mt10 -ep -hpVbDsLHSfbomQiQ6YuP7m1ZaNP0LQq
rar.exe	2216	39.57	C:/Windows/Temp/rar.exe a -df -m0 -mt10 -ep -hpVbDsLHSfbomQiQ6YuP7m1ZaNP0LQq
rar.exe	1340		C:/Windows/Temp/rar.exe a -df -m0 -mt10 -ep -hpVbDsLHSfbomQiQ6YuP7m1ZaNP0LQq
rar.exe	3252		C:/Windows/Temp/rar.exe a -df -m0 -mt10 -ep -hpVbDsLHSfbomQiQ6YuP7m1ZaNP0LQq
rar.exe	3404		C:/Windows/Temp/rar.exe a -df -m0 -mt10 -ep -hpVbDsLHSfbomQiQ6YuP7m1ZaNP0LQq

1. irudia. RAR1Ransom-ek egindako zifratze-prozesuak

Oraingoz, ransomware-kanpaina honen atzean dauden mehatxu-aktoreek badakigu 2 XMR (300 euro inguru) ordaintzeko eskatzen dietela biktimei, desenkriptatzailea emateko erabiltzaileei.

Azkenik, *Mirai* botnetari dagokionez, zerbitzua ukatzeko eraso banatuak eta indar gordineko erasoak egiten dira. Azken eraso horiek kontu eta pasahitz kodetuen bidez egiten dira.

Aurreko ahultasunak produktu hauei eragiten die:

- VMWare Workspace One Access 20.10.0.0 – 21.08.0.1 bertsioak

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 partxeak argitaratu bezain laster.

Neurriak azkar hartzea garrantzitsua da, inplementazioan arazo hori eten edo arintzeko. Horregatik, ahultasunaren larritasuna kontuan hartuta, VMWare-k proposatutako irtenbide ofiziala aplikatzea gomendatzen da. Lotura honetan dago:

- HW-154129 – Patch instructions to address CVE-2022-22954, CVE-2022-22955, CVE-2022-22956, CVE-2022-22957, CVE-2022-22958, CVE-2022-22959, CVE-2022-22960, CVE-2022-22961 in Workspace ONE Access Appliance.

Era berean, fabrikatzaileak ordezko arintzea eman die erabiltzaileei, honako urrats hauek gomendatuz:

- Saioa sshuser gisa hasi, sudo, root gisa sartzeko.
- HW-154129-applyWorkaround.py scripta deskargatu eta sistemara transferitzea, SCP protokoloa erabiltzea gomendagarria delarik.
- Deskargatutako fitxategiaren ibilbidera nabigatu cd komandoaren bidez.
- Python-en scripta exekutatu python3 HW-154129-applyWorkaround.py komandoa erabiliz.

4. Erreferentzia osagarriak

- NIST: CVE-2022-22954 Detail.
- CWE-94: Improper Control of Generation of Code ('Code Injection').
- Rar1 (.rar1) ransomware virus – removal and decryption options.
- Botnet: Mirai.
- Hacker exploit critical VMware flaw to drop ransomware, miner.
- Multiple Campaigns Exploit VMware Vulnerability to Deploy Crypto Miners and Ransomware.
- Mirai, RAR1Ransom, and GuardMiner – Multiple Malware Campaigns Target VMware Vulnerability.
- VMware warns of critical vulnerabilities in multiple products.
- Twitter: Bad Packets.
- Breach prevention blog.
- NIST: CVE-2021-31805 Detail.
- NIST: CVE-2022-26134 Detail.
- NIST: CVE-2022-22947 Detail.
- VMSA-2022-0011.
- HW-154129 – Patch instructions to address CVE-2022-22954, CVE-2022-22955, CVE-2022-22956, CVE-2022-22957, CVE-2022-22958, CVE-2022-22959, CVE-2022-22960, CVE-2022-22961 in Workspace ONE Access Appliance.
- HW-154129 - Workaround instructions to address CVE-2022-22954, CVE-2022-22955, CVE-2022-22956, CVE-2022-22957, CVE-2022-22958, CVE-2022-22959, CVE-2022-22960 in Workspace ONE Access Appliance.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA