PwnKit ahultasuna (CVE-2021-4034)

BCSC-AHULTASUNAK-PWNKIT

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

Joan den urtarrilaren 25ean, Qualys taldearen taldeak Polkit-eko pkexec memoria-ustelkeriaren ahultasuna argitaratu zuen, Linux-eko banaketa nagusietan modu lehenetsian instalatzen den SUIDeko root programa. Ahultasuna CVE-2021-4034 zenbakiarekin erregistratu da, baina PwnKit ere deitu zaio (polkit aplikazio kalteberaren izena duen hitz-jokoa).

Polkit (lehen PolicyKit deitua) Unixen antzeko sistema eragileetan sistema osoaren pribilegioak kontrolatzeko erabiltzen den osagaia da. Pribilegiorik gabeko prozesuak prozesuekin pribilegioekin komunikatzeko modu antolatu bat eskaintzen du. Pkexec komandoaren bidez pribilegio handiko komandoak exekutatzeko polkit-a erabil daiteke, eta, ondoren, administratzaile baimenekin exekutatu nahi den komandoa.

Ahultasun horren ustiapen arrakastatsuari esker, pribilegiorik gabeko edozein erabiltzailek administratzaile pribilegioak lor ditzake host kalteberan. Qualys segurtasun ikertzaileek modu independentean egiaztatu ahal izan dute ahultasuna, exploit bat garatu dute (ez dute publiko egin) eta root pribilegio osoak lortu Ubuntu, Debian, Fedora eta CentOS instalazioetan. Ez da baztertzen Linuxen beste banaketa batzuk kalteberak eta potentzialki ustiagarriak izatea. ahultasun hori 12 urte baino gehiagoan egon da ezkutuan, 2009ko maiatzean lehen bertsioa egin zenetik pkexec bertsio guztiei eragiten baitie.

Erraz ustiatzeko moduko ahultasuna da, ustiatzen laguntzen duten hainbat baldintza betetzen baititu. Alde batetik, Pkexec modu lehenetsian instalatuta dago Linuxen banaketa nagusietan, eta, gainera, komando kaltebera da 2009ko maiatzean sortu zenetik. Bestalde, pribilegiorik gabeko tokiko edozein erabiltzailek aukera du akatsa ustiatzeko eta root pribilegio osoak lortzeko. Era berean, kontuan izan behar da akats hori ustiagarria dela, baita polkit gauzatzen ez bada ere.

2. AZTERKETA TEKNIKOA

CVE-2021-4034 urrakortasunak polkit-eko pkexec komandoari eragiten dio, Unix-en antzeko sistema eragileetan sistema osoaren pribilegioak kontrolatzeko osagaia baita. Pkexec komandoaren bidez, erabiltzaile batek pribilegio handiko komandoak egin ditzake.

Ahultasuna pkexec-en main () funtzioaren printzipioaz baliatzen da. Funtzio horrek komando-lerroaren argudioak prozesatzen ditu eta, ibilbidea erabatekoa ez bada, PATH ingurunearen aldagaiaren direktorioetan exekutatu beharreko programa bilatzen du. Kontuan izan behar da argc komandoen lerroko argumentuen kopurua 0 bada (execve () ra igarotzen garen argv argudioen zerrenda hutsik badago, hau da, {NULL}), orduan argv [0] NULL da. Adibidez, PATH inguruneko aldagaia "Path = izena" bada, eta "izena" direktorioa existitzen bada eta "balioa" izeneko fitxategi exekutagarri bat badu, "Izena/balioa" kateko punta-puntako bat envp [0] mugetatik kanpo idazten da. Beste era batera esanda, mugetatik kanpoko idazkera honek aukera ematen digu ingurune "ez-seguruaren" aldagai bat (adibidez, LD_PRELOAD) berriz sartzeko pkexec-en. Aldagai "ez-seguru" horiek normalean (ld.so bidez) SUID programen ingurunetik ezabatzen dira main funtzioa exekutatu aurretik ().

Akats honen ustiapen arrakastatsua lortzeko, kontuan izan behar da akats mezu bat stderr inprimatzeko, pkexec-ek GLib (liburutegi GNOME) funtzioari deitzen diola. Adibidez, validar_environment_variable() funtzioak eta log_message () deitzen dute g_printerr (). g_printerr () normalean UTF-8 errore-mezuak inprimatzen ditu, baina mezuak beste karaktere-sorta batean inprimatu ditzake Charset ingurunearen aldagaia UTF-8 ez bada. UTF-8 mezuak beste txarset batera bihurtzeko, g_printerr () deitu glibc iconv_open() funtzioari. Karaktere multzo batetik bestera mezuak bihurtzeko, iconv_open () exekutatzen da liburutegi partekatu txikietan; normalean, hiruki horiek ("from" charset, "To" karaktere-jokoa eta liburutegiaren izena) aurretik zehaztutako konfigurazio-fitxategi batetik irakurtzen dira,/usr/lib/gconv/gconv-moduloa. Bestela, GCONV_PATH ingurunearen aldagaiak iconv_open () -a behartu dezake beste konfigurazio-fitxategi bat irakurtzera; Jakina, GCONV_PATH (ingurunearen aldagai "ez segurua", liburutegi arbitrarioak egikaritzera eramaten baitu) SUID programen ingurunetik ezabatzen da.

Zoritxarrez, CVE-2021-4034 aukera ematen dio erasotzaileari berriro GCONV_PATH pkexec ingurunean sartzeko, eta liburutegi partekatu bat exekutatzeko administratzaile gisa.

Qualissek ez zuen ustiapen-kodea zabaldu nahi izan, baina txostena argitaratu eta ordu gutxira exploit bat argitaratu zen. Esteka honetan ikus dezakezue CVE-2021-4034rako Python-en ustiapen-kodea.

3. ARINTZEA / KONPONBIDEA

Ohikoa denez, ahultasun hori eta beste batzuk prebenitzeko, BCSCtik gomendatzen da sistemak eta aplikazioak azken bertsio erabilgarrira eguneratuta izatea beti.

Polkit-en 2009tik aurrerako bertsio guztiak kalteberak direnez, administratzaileei gomendatzen zaie Polkit-en egileek beren GitLab-en publiko egin dituzten adabakiak aplikatzeari lehentasuna ematea.

Linuxen banaketa guztiak adabakira sartu ahal izan ziren urtarrilaren 25ean Qualissek dibulgazio koordinatua egin baino pare bat aste lehenago. Gainera, Ubuntuk Policykit-erako eguneratzeak bidali ditu, ahultasunari aurre egiteko 14.04 eta 16.04 ESM bertsioetan (segurtasun hedatuaren mantenimendua), baita 18.04, 20.04 eta 21.04 bertsio berrienetan ere. Erabiltzaileek sistemaren eguneratze estandarra exekutatu besterik ez dute egin behar, eta, ondoren, gailua berrabiarazi, aldaketek eragina izan dezaten. Red Hatek segurtasun-eguneraketa bat ere eman zuen polkit-erako Workstation-en eta Enterprise produktuetarako arkitektura bateragarrietarako, baita bizi-ziklo hedatuaren euskarrirako ere, TUS eta AUS.

Adabaki bat oraindik bidali ez duten sistema eragileak aldi baterako arintzea honako komando hau erabiltzea da, pkexec-i bit setuid kentzeko:

```
chmod 0755 /usr/bin/pkexec
```

4. ERREFERENTZIA OSAGARRIAK

- PwnKit: Local Privilege Escalation Vulnerability Discovered in polkit's pkexec (CVE-2021-4034)
- Qualys Security Advisory
- Linux system service bug gives root on all major distros, exploit released
- Linux distros haunted by Polkit-geist for 12+ years: Bug grants root access to any user
- SUID y SGID: Ejecutar un programa con permisos elevados
- Como establecer la variable PATH
- Python exploit code for CVE-2021-4034 (pwnkit)
- Extended Security Maintenance
- Mantenimiento de Seguridad Extendido
- Red Hat Enterprise Linux Telecommunications Update Service (TUS) Life Cycle
- What is Advanced mission critical Update Support (AUS)?
- Error de Codificacion UTF8

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?