Nro. Alerta:	EC-2021-033	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	11-dic-2021	**Vulnerabilidad de Ubuntu que permite escalar privilegios**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Vulnerable

Tipo de incidente: Sistemas y/o software abiertos

Nivel de riesgo: Alto

II. ALERTA

Investigador de GitHub descubrió que AccountsService de versiones de Ubuntu 21.10, Ubuntu 21.04 y Ubuntu 20.04 LTS, gestiona la memoria de manera incorrecta al realizar ciertas operaciones de configuración de idioma, vulnerabilidad que un atacante local podría usar este problema para escalar privilegios y tomar el control total.

Figura 1.- fallo de seguridad permite el escalamiento de privilegios de usuario en Ubuntu
Fuente: GitHub

III. INTRODUCCIÓN

Las modificaciones específicas de Ubuntu a accountsservice (en el archivo de parche debian / patches / 0010-set-language.patch) hicieron que la variable fallback_locale, que apunta al almacenamiento estático, se libere, en la función

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

user_change_language_authorized_cb. Esto es accesible a través de la función dbus SetLanguage.

Figura 2.- Gravedad de la vulnerabilidad CVE-2021-3939
Fuente: NIST

IV. VECTOR DE ATAQUE: Local

AccountsService es un servicio de D-Bus que ayuda a manipular y consultar información adjunta a las cuentas de usuario disponibles en un dispositivo.

El investigador de seguridad Kevin Backhouse, detectó accidentalmente la falla de seguridad (un error de administración de memoria registrado como CVE-2021-3939) mientras probaba una demostración de exploits para otro error de AccountsService que también hizo posible escalar privilegios a root en dispositivos vulnerables.

El concepto básico es convertir la vulnerabilidad de doble libre en un error de uso después de libre, como se muestra en este diagrama:

Nro. Alerta:	EC-2021-033	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	11-dic-2021	**Vulnerabilidad de Ubuntu que permite escalar privilegios**	V 1.1

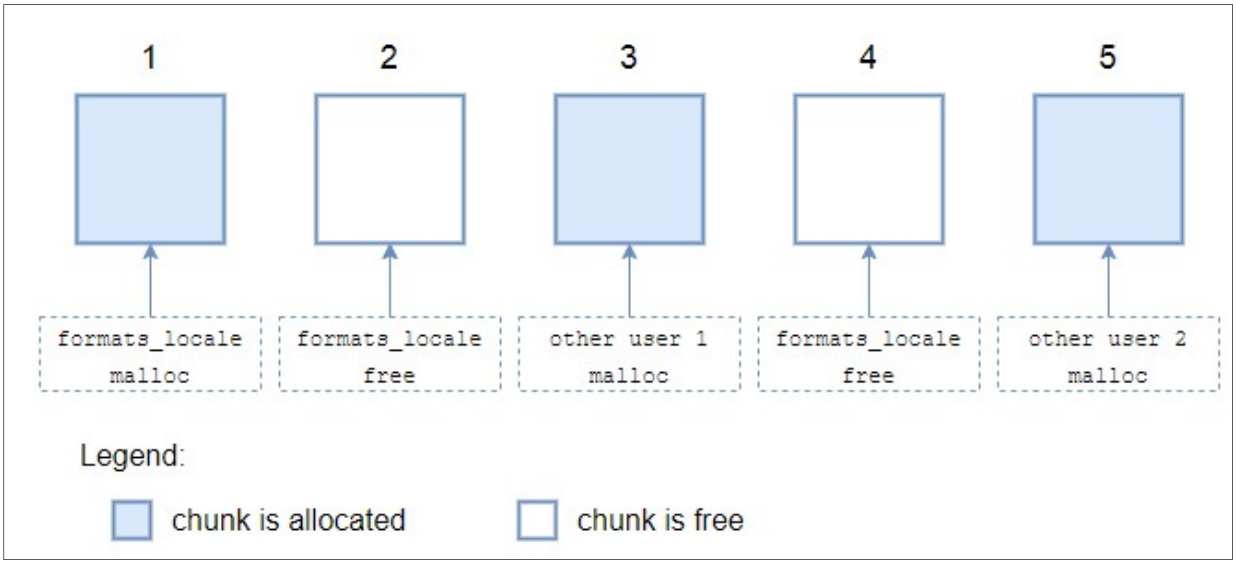

Figura 2 Cómo explotar un error sin doble
Fuente: github

Estos son los pasos:

- Se asigna una parte de la memoria (y se almacena system_formats_locale).
- El error se activa y el fragmento se libera (dejando un puntero colgando system_formats_locale).
- La memoria se asigna en alguna otra parte del código y obtiene un puntero al mismo fragmento al que ya pertenece system_formats_locale.

Dos "propietarios" creen que poseen el mismo fragmento de memoria. En algunos escenarios de explotación, esto puede ser suficiente para explotar el error: si uno de los propietarios cambia el contenido del fragmento, es posible que se engañe al otro propietario para que haga algo incorrecto. Sin embargo, en el caso específico de CVE-2021-3939, no es suficiente porque system_formats_locale es un puntero de solo lectura que no se usa para nada particularmente interesante. Pero está bien, porque puedo activar el error dos veces:

El error se activa de nuevo y el fragmento se libera por segunda vez.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2021-033	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	11-dic-2021	**Vulnerabilidad de Ubuntu que permite escalar privilegios**	V 1.1

Otra parte del código asigna algo de memoria y también obtiene un puntero al mismo fragmento.
Ahora hay tres "propietarios" separados que piensan que poseen el mismo fragmento de memoria. Si el "usuario 1" sobrescribe el fragmento, entonces el "usuario 2" podría hacer algo incorrecto, o viceversa.

V. IMPACTO:

Según el investigador de seguridad, al explotar la vulnerabilidad se puede bloquear el AccountsService (Sistema de los usuarios) o ejecutar programas con permisos de administrador al obtener acceso root.

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente expuesto por el fabricante:

- Actualizar su sistema a las siguientes versiones del paquete:

  Ubuntu 21.10
  Servicio de cuentas - 0.6.55-0ubuntu14.1
  libaccountsservice0 - 0.6.55-0ubuntu14.1

  Ubuntu 21.04
  Servicio de cuentas - 0.6.55-0ubuntu13.3
  libaccountsservice0 - 0.6.55-0ubuntu13.3

  Ubuntu 20.04
  Servicio de cuentas - 0.6.55-0ubuntu12 ~ 20.04.5
  libaccountsservice0 - 0.6.55-0ubuntu12 ~ 20.04.5

- Después de una actualización estándar del sistema, reiniciar el computador para realizar todos los cambios necesarios.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2021-033	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	11-dic-2021	**Vulnerabilidad de Ubuntu que permite escalar privilegios**	V 1.1

VII. REFERENCIAS:

Backhouse, K. (13 de diciembre de 2021). *GitHub*. Obtenido de https://securitylab.github.com/research/ubuntu-accountsservice-CVE-2021-3939/

Jiménez, J. (14 de diciembre de 2021). *RedesZone*. Obtenido de https://www.redeszone.net/noticias/seguridad/fallo-permisos-root-ubuntu/

Nist. (16 de noviembre de 2021). *Nist*. Obtenido de https://nvd.nist.gov/vuln/detail/CVE-2021-3939#vulnCurrentDescriptionTitle

Ubuntu. (16 de noviembre de 2021). *Ubuntu*. Obtenido de https://ubuntu.com/security/notices/USN-5149-1

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec