Vulnerabilidad en SUDO

BCSC-Vulnerabilidad-SUDO

TLP:WHITE

www.basquecybersecurity.eus

Enero 2021

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

SOBRE EL BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

1. RESUMEN EJECUTIVO

Investigadores de seguridad de la empresa Qualys han alertado sobre una vulnerabilidad crítica en la utilidad **SUDO**, presente en casi la totalidad de sistemas operativos basado en **Unix** y **Linux**. Este programa permite ejecutar instrucciones con los privilegios de seguridad del usuario root (usuario que tiene acceso administrativo al sistema) siempre y cuando se tengan privilegios o se conozca la contraseña de dicho usuario. Debido al fallo detectado, cualquier usuario local podría obtener privilegios de usuario root en un equipo o dispositivo vulnerable comprometiendo así la seguridad del sistema.

Esta vulnerabilidad conocida como "*Baron Samedit*" produce, según los investigadores, un **desbordamiento de búfer** que puede explotar cualquier usuario sin privilegios permitiendo obtener privilegios de usuario root en múltiples sistemas operativos **Linux** entre los que se encuentran algunos de los más extendidos como **Debian**, **Ubuntu** y **Fedora**.

Los propios investigadores de **Qualys** que han reportado el fallo también han participado en la divulgación responsable de la vulnerabilidad y se han coordinado con los colaboradores de **SUDO** y las distribuidoras de código abierto para anunciar su resolución mediante parches en una **nueva versión** de **SUDO** lanzada el pasado día 26 de enero de 2021. Por tanto, aquellos administradores de sistemas que usen SUDO para otorgar privilegios de usuario root a sus usuarios locales deben aplicar la actualización en cuanto sea posible.

2. ANÁLISIS TÉCNICO

La utilidad **SUDO** se encuentra presente en casi la totalidad de los sistemas operativos basados en **Unix** y **Linux** permitiendo a los administradores del sistema proporcionar privilegios de ***root*** limitados a los usuarios normales que figuran en el archivo *sudoers*, mientras que al mismo tiempo mantienen un registro de su actividad. El programa funciona según el principio de privilegio mínimo, otorgando a los usuarios los permisos necesarios para realizar su trabajo sin comprometer la seguridad general del sistema. Al ejecutar comandos en un sistema operativo, los usuarios sin privilegios pueden usar el comando "**sudo**" (*superuser do*) para ejecutar comandos como ***root*** si tienen permiso o conocen la contraseña del usuario ***root***, el cual es el superusuario del sistema, es decir, una cuenta especial de administración del sistema.

Según las investigaciones, esta vulnerabilidad ha estado presente en **SUDO** durante casi 10 años afectando a múltiples de sus versiones en sus configuraciones predeterminadas.

Conocida como "*Baron Samedit",* ha sido identificada con el **CVE-2021-3156** y definida como un **desbordamiento de búfer** que permite elevar privilegios a ***root*** mediante el comando "*sudoedit -s*" y un argumento de línea de comandos que finaliza con un sólo carácter de barra invertida. Además, el fallo es explotable por cualquier usuario local y no requiere conocer la contraseña de ningún usuario del sistema para que el ataque sea exitoso.

En concreto, el desbordamiento de búfer es posible ya que SUDO **elimina de forma incorrecta las barras diagonales inversas en los argumentos**. Tal y como se puede leer en el registro de cambios de la nueva versión 1.9.5p2 de la propia utilidad, "…*Normalmente, SUDO evita los caracteres especiales cuando se ejecuta un comando a través de un shell (sudo -s o sudo -i)…*", pero las investigaciones han demostrado que también era posible ejecutar "*sudoedit"* con los indicadores *-s* o *-i*, en cuyo caso no se habrían evitado los caracteres, haciendo posible el desbordamiento de memoria.

Los analistas que han reportado esta vulnerabilidad, han llegado a crear hasta **3 exploits** diferentes con los que se logra su explotación en múltiples distribuciones de **Linux** como **Debian 10 (Sudo 1.8.27)**, **Ubuntu 20.04 (Sudo 1.8.31)** y **Fedora 33 (Sudo 1.9.2)**.

Así mismo, han publicado un video con una prueba de concepto sobre la explotación del fallo:

- https://vimeo.com/504872555

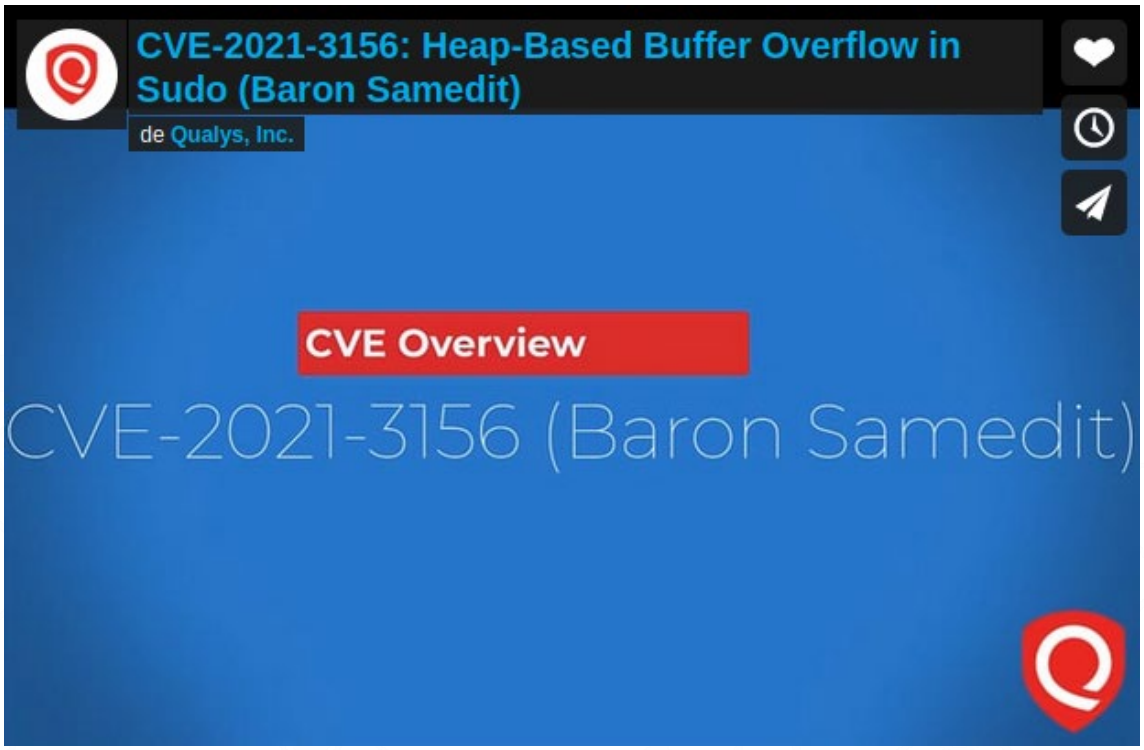

Ilustración 1. PoC CVE-2021-3156 (Baron Samedit)

3. MITIGACIÓN / SOLUCIÓN

Cabe destacar que esta vulnerabilidad ya se notificó a **SUDO** hace casi 10 años, en julio de 2011 bajo la referencia 8255ed69, y afecta a las configuraciones predeterminadas de todas sus versiones estables desde la **1.9.0** a la **1.9.5p1** y a todas las versiones heredadas desde la **1.8.2** a la **1.8.31p2**.

La vulnerabilidad ya ha sido solucionada en la nueva versión de **SUDO 1.9.5p2** publicada recientemente por lo que en caso de hacer uso de **SUDO** para otorgar privilegios de ***root*** a usuarios, se debe aplicar esta nueva versión o posterior en cuanto sea posible:

- https://www.sudo.ws/dist/sudo-1.9.5p2.tar.gz

Para comprobar si un sistema es vulnerable, se debe iniciar sesión como usuario **no root** y ejecutar el comando "*sudoedit -s /*". Un sistema vulnerable arrojará un error que comienza con "*sudoedit:*", mientras que un sistema con la última versión de **SUDO** parcheada mostrará un mensaje que comenzará con "*usage:*". Además, conviene recordar que la vulnerabilidad es explotable bajo **configuraciones predeterminadas de SUDO**, lo que aumenta considerablemente el riesgo de sufrir ataques que aprovechen este error:

Ilustración 2. Error mostrado por un sistema vulnerable

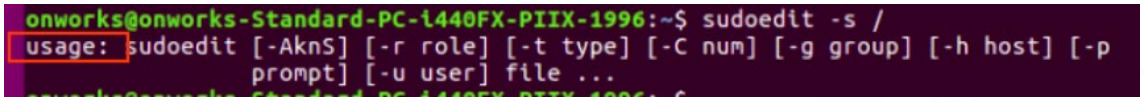

Ilustración 3. Salida al comando ejecutado en un sistema no vulnerable

4. REFERENCIAS ADICIONALES

- Baron Samedit: Heap-based buffer overflow in Sudo (CVE-2021-3156)
- Buffer overflow in command line unescaping
- sudo: Multiple vulnerabilities — GLSA 202101-33

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?