BOLETÍN DE ALERTA

Boletín Nro.: 2019-04
Fecha de publicación: 14/10/2019
Tema: Vulnerabilidad crítica en sudo podría permitir a un atacante evadir las restricciones Runas y ejecutar comandos como root.

- CVE-2019-14287

Sistemas afectados:

Todas las versiones de sudo anteriores a la 1.8.28 se ven afectadas.

Descripción:

Una vulnerabilidad en Sudo, una de las utilidades más relevantes de Linux, permite ejecutar comandos con acceso raíz, incluso cuando estos no están autorizados por el usuario. Dicha vulnerabilidad omite la política de seguridad de sudo, permitiendo así que otros usuarios o programas ejecuten comandos root.

Cuando sudo es configurado para permitir a los usuarios ejecutar comandos arbitrarios mediante el parámetro ALL en Runas, es posible ejecutar comandos como root empleando los ID de usuario -1 o 4294967295.

Esto se debe a que la función que convierte la identificación de usuario en su nombre de usuario trata incorrectamente -1 o su equivalente no firmado 4294967295, como 0, que siempre es la identificación de usuario raíz.

Impacto:

La vulnerabilidad permite que cualquier usuario atacante logre identificarse como root, evadiendo las restricciones de usuarios de Runas en el sistema, y tomar el control completo sobre el sistema, pudiendo realizar modificaciones.

Solución:

La versión estable actual y que corrige esta vulnerabilidad es sudo 1.8.28, lanzada el 14 de octubre de 2019. Se recomienda instalar lo antes posible la última versión disponible.

Prevención:

Para conocer el estado de seguridad detallado de sudo, consulte su página de seguimiento de seguridad en forma periódica.

Información adicional:
https://www.sudo.ws/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14287
https://www.sudo.ws/alerts/minus_1_uid.html
https://www.debian.org/security/2019/dsa-4543#DSAS
https://access.redhat.com/security/cve/cve-2019-14287
https://people.canonical.com/~ubuntu-security/cve/2019/CVE-2019-14287.html