BOLETÍN DE ALERTA

Boletín Nro.: 2020-04

Fecha de publicación: 04/02/2020

Tema: Vulnerabilidad en sudo permitiría escalar privilegios de usuarios.

- CVE-2019-18634

Sistemas afectados:

- Todas las versiones de la utilidad sudo anteriores a la 1.8.31, en macOS y sistemas operativos basados en UNIX o Linux.

Descripción:

La vulnerabilidad puede ser explotada cuando la función **pwfeedback** está habilitada en el archivo de configuración de sudoers ***/etc/sudoers.***

La opción **pwfeedback** de sudo, ofusca la contraseña cuando está siendo ingresada por el usuario, es decir imprime un asterisco (*) en lugar de los caracteres de la contraseña, y si bien esta opción no se encuentra habilitada de manera predeterminada, algunos administradores de sistemas deciden habilitarlos. Además en algunos sistemas operativos como, Linux Mint y Elementary OS, esta opción se encuentra habilitada por defecto.

Esta falla causa un **buffer overflow** (desbordamiento de memoria basado en pila) y se da en la función **getln()** de **tgetpass.c** cuando se ingresa una longitud de caracteres demasiado grande como contraseña, este no cabe en el búfer asignado y reescribe otros datos en la pila, provocando el conocido **buffer overflow**.

```
20 ■■■■■ src/tgetpass.c
@@ -61,7 +61,7 @@ enum tgetpass_errval {
    static volatile sig_atomic_t signo[NSIG];

    static void tgetpass_handler(int);
-   static char *getln(int, char *, size_t, int, enum tgetpass_errval *);
    static char *sudo_askpass(const char *, const char *);
```

Un ejemplo de explotación sería:

```
perl -e 'print(("A" x 100 . "\x{00}") x 50)' | sudo -S id

Password: Segmentation fault
```

Impacto:

Esta vulnerabilidad podría permitir a un atacante remoto con un usuario de pocos privilegios, y que no pertenezca al grupo de “sudoers” y/o a programas maliciosos, evadir las restricciones de usuarios en el sistema, y tomar el control completo del mismo, pudiendo ejecutar comandos arbitrarios con privilegios de root en sistemas Linux o macOS.

Solución y Prevención

- Actualizar sudo a la versión 1.8.31, disponible en el sitio oficial.
    - Como solución alternativa, Comprobar si la función **pwfeedback** está habilitada: ejecutar el comando "sudo -l" en su terminal Linux o macOS.
    - Desactivar la opción **pwfeedback** de sudo, para asegurar que el ataque ya no sea posible:
        - en el directorio **/etc/sudoers** localizar el archivo **pwfeedback**, luego abrir el archivo **pwfeedback** y reemplazar **“Defaults pwfeedback”** por **“Defaults !pwfeedback”.**

- En el caso de productos Apple, la semana pasada lanzó una actualización de parches que resuelven el problema para:
    - macOS High Sierra 10.13.6.
    - macOS Mojave 10.14.6.
    - macOS Catalina 10.15.2.

Información adicional:

- https://www.sudo.ws/security.html
- https://www.sudo.ws/alerts/pwfeedback.html
- https://vuldb.com/?id.149517
- https://thehackernews.com
- https://access.redhat.com/security/cve/cve-2019-18634
- https://www.debian.org/security/2020/dsa-4614
- https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2019-18634