I. DATOS GENERALES:

Clase de alerta: Informativo

Tipo de Incidente: Ejecución Arbitraria de Comandos | Escalamiento de Privilegios

Nivel de riesgo: Alta

II. ALERTA

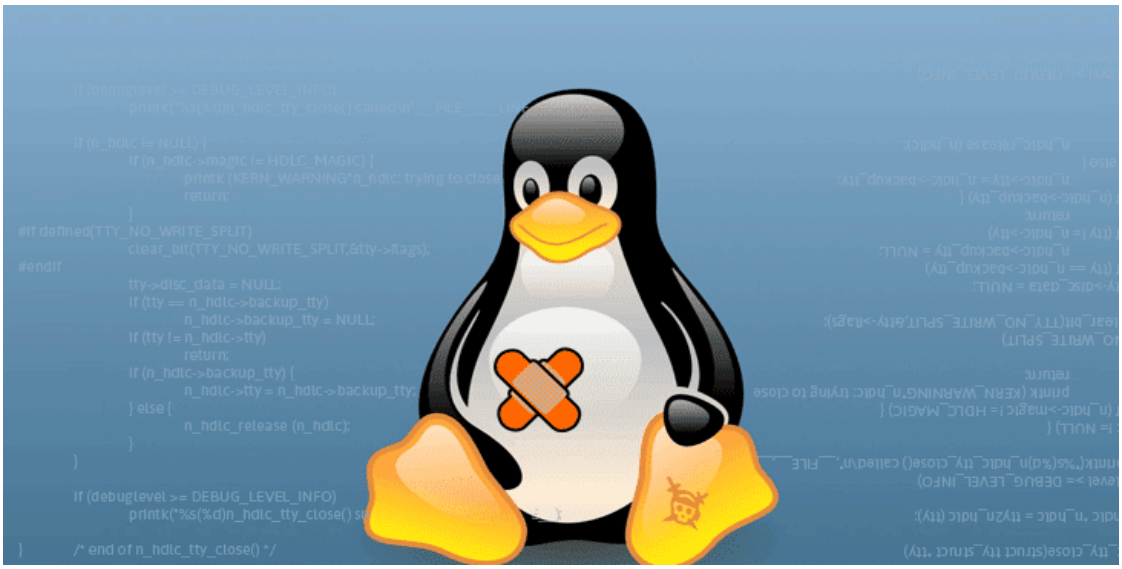

Figura 1.- Vulnerabilidad en Sudo (CVE-2025-32463) - figura referencial

Vulnerabilidad de distribuciones Linux encontrada bajo CVE-2025-32463 de ser explotada, podría permitir a un atacante ejecutar comandos arbitrarios con escalamiento de privilegios root.

III. INTRODUCCIÓN

Esta vulnerabilidad crítica de seguridad se encuentra en la utilidad Sudo de Linux, ampliamente utilizada, que permite a cualquier usuario local no privilegiado escalar de privilegios para el acceso a root.

El usuario necesita autenticarse con su contraseña y, si está permitido por el archivo de configuración sudoers (archivo de configuración en sistemas Unix/Linux que define qué usuarios o grupos tienen permisos para ejecutar comandos con privilegios elevados como superusuario o root, normalmente en /etc/sudoers), el sistema ejecutará el comando solicitado.

La vulnerabilidad se centra alrededor de la opción -R (chroot) de Sudo, que permite que usuarios sin privilegios invoquen chroot( ) en rutas modificables y no confiables bajo su control, las cuales Sudo ejecuta con permisos de root (superusuario).

Esto genera una brecha de seguridad cuando se activan operaciones del Name Service Switch (NSS), haciendo que el sistema cargue la configuración de /etc/nsswitch.conf desde el entorno no confiable.

En conclusión, el problema surge al permitir que un usuario no privilegiado invoque chroot( ) en una ruta escribible y no confiable bajo su control. Sudo llama a chroot( ) varias veces, independientemente de si el usuario tiene configurada una regla de Sudo correspondiente.

IV. VECTOR DE ATAQUE

El CVSS:3.1 le asigna una puntuación de 9.3 y determina con un tipo de ataque Local CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

V. IMPACTO

La vulnerabilidad tiene su impacto en sistemas que soportan /etc/nsswitch.conf, un usuario podría ser capaz de ejecutar comandos arbitrarios como root.

Así como también se ha verificado la explotación en:

- Ubuntu 24.04.1; Sudo 1.9.15p5, Sudo 1.9.16p2
- Fedora 41 Server; Sudo 1.9.15p5
- Las versiones antiguas de Sudo (<= 1.8.32 que no son vulnerables porque la funcionalidad chroot no existe)

VI. INDICADORES DE COMPROMISO

Local user account (unprivileged): acceso a directorio grabable; no se requieren permisos de Sudo existentes; la configuración de Sudo predeterminada es suficiente.

VII. RECOMENDACIONES:

- Instalar los últimos paquetes de Sudo (el error está corregido en Sudo 1.9.17p1 y versiones posteriores).
- Evitar el uso de la opción chroot de no implementarlo correctamente.

- Buscar en su entorno cualquier uso de la opción chroot.
- Revisar todas las reglas de Sudo definidas en /etc/sudoers, así como los archivos en /etc/sudoers.d.
- Si las reglas de Sudo están almacenadas en LDAP, utilizar herramientas como ldapsearch para extraer las reglas.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

CVEDETAILS (2025). Vulnerability Details: CVE-2025-32463. https://www.cvedetails.com/cve/CVE-2025-32463/

NVD (2025). CVE-2025-32463 Detail. https://nvd.nist.gov/vuln/detail/CVE-2025-32463

UBUNTU (2025). CVE-2025-32463. https://ubuntu.com/security/CVE-2025-32463

REDHOTCYBER (2025). Linux PWNED: Privilege Escalation on Sudo in 5 Seconds – HackerHood tests the CVE-2025-32463 exploit. https://www.redhotcyber.com/en/post/linux-pwned-privilege-escalation-on-sudo-in-5-seconds-hackerhood-tests-the-cve-2025-32463-exploit/

HELPNETSECURITY (2025). Sudo local privilege escalation vulnerabilities fixed (CVE-2025-32462, CVE-2025-32463). https://www.helpnetsecurity.com/2025/07/01/sudo-local-privilege-escalation-vulnerabilities-fixed-cve-2025-32462-cve-2025-32463/

CYBERSECURITYNEWS (2025). Linux Sudo chroot vulnerability. https://cybersecuritynews.com/linux-sudo-chroot-vulnerability/