Boletín de alerta

Boletín Nro.:
Fecha de publicación: 12/08/2025
Tema: Alerta 2025-67 Multiple Vulnerabiliades CyberArk Secret Manager
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

CyberArk Secret Manager (originalmente conocido como Conjour Enterprise):

- Versiones de la 13.1 a la 13.6.

Descripción

Se han reportado múltiples vulnerabilidades en productos CyberArk:

- **CVE-2025-49827 [CVSS 9.1, Crítico]:** Omisión del autenticador de IAM en Secrets Manager, alojado en el sistema (anteriormente Conjur Enterprise) y Conjur OSS
- **CVE-2025-49831 [CVSS 9.1, Crítico]:** Omisión del autenticador de IAM mediante un dispositivo de red mal configurado en Secrets Manager, alojado en el sistema (anteriormente Conjur Enterprise) y Conjur OSS
- **CVE-2025-49828 [CVSS 8.6, Alto]:** Ejecución remota de código en Secrets Manager, alojado en el sistema (anteriormente Conjur Enterprise) y Conjur OSS
- **CVE-2025-49830 [CVSS 7.1, Alto]:** Recorrido de rutas y divulgación de archivos en Secrets Manager, alojado en el sistema (anteriormente Conjur Enterprise) y Conjur OSS
- **CVE-2025-49829 [CVSS 6.0, Moderado]:** Validaciones faltantes en Secrets Manager, Self-Hosted (anteriormente Conjur Enterprise) y Conjur OSS

La combinación de estas vulnerabilidades permite que un atacante no autenticado ejecute código arbitrario en el sistema objetivo sin necesidad de una contraseña, un token o credenciales de AWS**.**

CVE-2025-49827 es una vulnerabilidad crítica de omisión de autenticación de IAM. Su explotación podría permitir que un atacante remoto, capaz de manipular los encabezados firmados por AWS, aproveche una expresión regular malformada para redirigir la solicitud de validación de autenticación que Secrets Manager, Self-Hosted, envía a AWS a un servidor malicioso controlado por el atacante.

La vulnerabilidad crítica, **CVE-2025-49831, también implica la omisión del autenticador de IAM mediante un dispositivo de red mal** configurado en Secrets Manager, Self-Hosted y Conjur OSS. Su explotación

exitosa podría permitir que un atacante redirija las solicitudes de autenticación a un servidor malicioso bajo su control.

CVE-2025-49828 es una vulnerabilidad de ejecución remota de código (RCE). Un atacante autenticado que pueda inyectar secretos o plantillas en la base de datos de Secrets Manager, Self-Hosted, podría aprovechar un endpoint de API expuesto para ejecutar código arbitrario dentro del proceso de Secrets Manager.

CVE-2025-49830 es una vulnerabilidad de cruce de rutas y divulgación de archivos. Un atacante autenticado capaz de cargar la política puede usar el analizador YAML de la política para referenciar archivos en el servidor alojado en el propio Secrets Manager. Estas referencias pueden usarse con fines de reconocimiento para comprender mejor la estructura de carpetas del servidor Secrets Manager/Conjur o para que el analizador YAML incluya archivos del servidor en el YAML que se procesa al cargar la política.

Mitigación:

Se recomienda encarecidamente instalar actualizaciones para dispositivos vulnerables con la máxima prioridad, después de realizar pruebas exhaustivas. Las vulnerabilidades ya no se encuentran presente en la versión 13.6.1.

Información adicional:

- https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2025-49827
- https://thehackernews.com/2025/08/cyberark-and-hashicorp-flaws-enable.html?m=1
- https://www.cyberark.com/resources/product-insights-blog/addressing-recent-vulnerabilities-and-our-commitment-to-security
- https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2025-49828