Boletín de alerta

Boletín Nro.:
Fecha de publicación: 06/02/2026
Tema: Alerta 2026-12 Vulnerabilidad Critica n8n
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

Se identificaron vulnerabilidades críticas que afectan a la plataforma de automatización de flujos de trabajo **n8n**, incluyendo:

- Versiones **anteriores a 1.123.17**
- Versiones **anteriores a 2.5.2**
- Implementaciones **n8n Cloud**
- Implementaciones **on-premise (autogestionadas)**

Descripción

Se identificó la vulnerabilidad **CVE-2026-25049**, clasificada con una severidad **Crítica (CVSS 3.1: 10.0)**, que afecta a la plataforma n8n. Investigadores de Pillar Security detectaron que esta falla permite que cualquier usuario autenticado obtenga control total del servidor donde se ejecuta la solución.

La explotación de esta vulnerabilidad podría permitir a un atacante ejecutar comandos arbitrarios, acceder a variables de entorno sensibles, incluyendo claves de cifrado, y descifrar credenciales almacenadas como claves API, tokens OAuth, contraseñas de bases de datos y accesos a proveedores de servicios en la nube.

En entornos **n8n Cloud**, debido a su arquitectura multiinquilino, un atacante podría potencialmente comprometer la infraestructura compartida, accediendo a información perteneciente a múltiples clientes. Además, la vulnerabilidad permite el acceso a archivos de configuración, manipulación de flujos automatizados, intercepción de procesos de inteligencia artificial y acceso a servicios internos dentro de entornos Kubernetes

Solución:

Actualizar a la versión **1.123.17, 2.5.2 o superior**

Información adicional:

- https://www.pillar.security/blog/n8n-sandbox-escape-critical-vulnerabilities-in-n8n-exposes-hundreds-of-thousands-of-enterprise-ai-systems-to-complete-takeover
- https://www.securityweek.com/critical-n8n-sandbox-escape-could-lead-to-server-compromise/
- https://thehackernews.com/2026/02/critical-n8n-flaw-cve-2026-25049.html