Boletín de alerta

Boletín Nro.:
Fecha de publicación: 07/01/2026
Tema: Alerta 2026-02 Vulnerabilidad Crítica en n8n
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- **n8n (Workflow Automation Platform)** en **todas las versiones iguales o anteriores a la 1.65.0**

Descripción

n8n es una plataforma de **automatización de flujos de trabajo** (workflow automation) de código abierto que permite **conectar aplicaciones, sistemas y servicios entre sí sin necesidad de programar** (o con muy poco código).

Se identificó la vulnerabilidad **CVE-2026-21858 (CVSS 10.0 – Crítica)**, conocida como *Ni8mare*, que permite a un atacante no autenticado tomar el control total de servidores n8n vulnerables, debido a que la plataforma procesa cargas de archivos sin validar correctamente el encabezado *Content-Type*; esta falla permite manipular solicitudes para copiar cualquier archivo local del sistema, exponiendo secretos, credenciales y tokens administrativos, así como ejecutar comandos remotos en el servidor, lo que puede derivar en robo de información, acceso administrativo no autorizado, ejecución de código arbitrario y compromiso completo del sistema, afectando potencialmente a más de 100,000 servidores a nivel mundial.

Explicación técnica más detallada:

https://www.cyera.com/research-labs/ni8mare-unauthenticated-remote-code-execution-in-n8n-cve-2026-21858

Solución:

- **Actualizar n8n a la versión 1.121.0 o superior**
  (Recomendado usar la versión más reciente disponible)

Información adicional:

- https://thehackernews.com/2026/01/critical-n8n-vulnerability-cvss-100.html

https://www.cyera.com/research-labs/ni8mare-unauthenticated-remote-code-execution-in-n8n-cve-2026-21858