Boletín de alerta

Boletín Nro.: 78
Fecha de publicación: 28/07/2026
Tema: Alerta 2026-78 Vulnerabilidad Crítica de ejecución remota de commandos en n8n
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- n8n versiones anteriores a **1.123.22**; versiones **2.0.0** hasta **2.9.2; y** versión **2.10.0**

Descripción

Recientemente, el equipo de n8n publicó una nueva vulnerabilidad crítica identificada como **CVE-2026-27577**, la cual corrige vulnerabilidades adicionales descubiertas tras la divulgación de CVE-2025-68613. n8n es una plataforma de automatización de flujos de trabajo ampliamente utilizada para integrar aplicaciones, APIs y servicios mediante procesos automatizados. La vulnerabilidad posee una puntuación **CVSS v3.1 de 9.9 (CRÍTICA),** debido a que permite la ejecución remota de comandos sobre el sistema anfitrión con privilegios del proceso que ejecuta n8n.

El problema reside en el mecanismo de **evaluación de expresiones (Expression Evaluation)** utilizado por n8n para procesar parámetros dinámicos dentro de los flujos de trabajo. Un usuario autenticado con permisos para crear o modificar workflows puede construir expresiones especialmente diseñadas que logran escapar de las restricciones previstas por la plataforma y provocar la ejecución de comandos arbitrarios directamente en el sistema operativo. **La vulnerabilidad afecta a las implementaciones self-hosted** de n8n que ejecuten versiones vulnerables. En el caso de los clientes que utilizan n8n Cloud (SaaS), el fabricante indicó que las instancias del servicio fueron actualizadas de manera proactiva, por lo que no es necesario realizar acciones adicionales por parte de los usuarios del servicio administrado.

Aunque la explotación requiere autenticación, el impacto continúa siendo extremadamente elevado debido a que, en numerosos entornos empresariales, múltiples usuarios poseen privilegios para desarrollar o modificar flujos de automatización. Un atacante que comprometa una cuenta con estos permisos podría obtener ejecución de código en el servidor, comprometer credenciales, acceder a información sensible, instalar malware, desplazarse lateralmente dentro de la red o utilizar el servidor de automatización como punto de apoyo para ataques posteriores.

Esta vulnerabilidad corresponde a la debilidad CWE-94 (Improper Control of Generation of Code / Code Injection). La corrección incorpora restricciones adicionales al motor de evaluación de expresiones para

impedir que estas construcciones puedan derivar en ejecución de comandos del sistema.

Solución:

La principal recomendación consiste en actualizar inmediatamente a una versión corregida, misma que pueden encontrarse en el siguiente enlace: **Detalles y parches de la CVE-2026-27577**

• 1.123.22 o superior
• 2.9.3 o superior
• 2.10.1 o superior

Si la actualización no puede realizarse de forma inmediata, el fabricante recomienda aplicar las siguientes medidas temporales:

• Restringir la creación y modificación de workflows únicamente a usuarios completamente confiables.
• Aplicar el principio de mínimo privilegio a las cuentas que ejecutan n8n.
• Ejecutar n8n dentro de entornos aislados (contenedores o máquinas virtuales) con permisos limitados.
• Restringir el acceso del servidor mediante segmentación de red y controles de firewall.
• Limitar los privilegios del sistema operativo y el acceso a recursos críticos para reducir el impacto de una posible explotación.
• El fabricante enfatiza que estas medidas no eliminan la vulnerabilidad, únicamente reducen el riesgo hasta que sea posible instalar las versiones corregidas.

Información adicional:

- **NVD – CVE-2026-27577**
  https://nvd.nist.gov/vuln/detail/CVE-2026-27577
- **GitHub Security Advisory (GHSA-vpcf-gvg4-6qwr)**
  https://github.com/n8n-io/n8n/security/advisories/GHSA-vpcf-gvg4-6qwr
- **GitHub Security Advisory (GHSA-v98v-ff95-f3cp)**
  https://github.com/n8n-io/n8n/security/advisories/GHSA-v98v-ff95-f3cp
- **Guía de seguridad de n8n**
  https://docs.n8n.io/hosting/securing/overview