

Boletín de alerta

Boletín Nro.:

Fecha de publicación: 19/05/2025

Tema: Alerta 2025-43- Falla Crítica en NodeJS

Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Node JS: versiones 20.x, 22.x, 23.x y 24.x.

Descripción

Se han reportado **tres vulnerabilidades en el producto NodeJS, una de ellas marcada como importante**, que podrían afectar seriamente la estabilidad y seguridad de las aplicaciones que usan este entorno de ejecución. Las mismas fueron identificadas como: CVE-2025-23166 con score 7.5, CVE-2025-23167 con score 6.5 y CVE-2025-23165 con score 3.5

Estas fallas pueden ser utilizadas por atacantes para **bloquear servidores, saltarse controles de acceso o generar fugas de memoria**, provocando interrupciones en servicios que dependen de Node.js.

A continuación se detallan las mismas:

- CVE-2025-23166 – Falla crítica en operaciones criptográficas asíncronas

Un error en el manejo de entradas no confiables puede permitir a un atacante bloquear remotamente una aplicación Node.js, afectando la disponibilidad del servicio (Denegación de Servicio o DoS).

- CVE-2025-23167 – Vulnerabilidad en encabezados HTTP (contrabando de solicitudes)

Una mala validación de encabezados HTTP podría permitir a los atacantes eludir controles de seguridad implementados a través de proxies.

- CVE-2025-23165 – Fuga de memoria en el sistema de archivos

Una falla en la función ReadFileUtf8 puede provocar un uso excesivo de memoria, lo que eventualmente lleva al sistema a fallar por agotamiento de recursos.

Solución:

El equipo de NodeJS ha publicado parches de seguridad que corrigen estas vulnerabilidades de acuerdo a la rama:

- [Node.js v20.19.2](#)
- [Node.js v22.15.1](#)
- [Node.js v23.11.1](#)
- [Node.js v24.0.2](#)

Información adicional:

- <https://feedly.com/cve/CVE-2025-23166>
- <https://securityonline.info/node-js-alerts-high-severity-flaw-cve-2025-23166-risks-remote-system-crashes-update-immediately/>
- <https://nodejs.org/en/blog/vulnerability/may-2025-security-releases>
- <https://nodejs.org/es/download>