BOLETÍN DE ALERTA

Boletín Nro.: 2023-02
Fecha de publicación: 10/01/2023
Tema: Vulnerabilidad de ejecución remota de código (*RCE*) en librería node-jsonwebtoken (*JWT*).

El producto afectado es:

- node-jsonwebtoken, versión 8.5.1 y anteriores.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad que afecta a la librería node-jsonwebtoken (*JWT*), que permitiría a un atacante realizar ejecución remota de código (*RCE*) en el sistema afectado. Actualmente existe una prueba de concepto (*PoC*) pública.

La vulnerabilidad identificada como CVE-2022-23529, de severidad "crítica", con una puntuación asignada de 9.8. Esta vulnerabilidad se debe a una falla de seguridad en el método *verify()* de node-jsonwebtoken. Esto permitiría a un atacante a través de un token JWS especialmente diseñado enviado a la víctima realizar ejecución remota de código (*RCE*) y provocar divulgación de información confidencial en el sistema afectado.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante realizar ejecución remota de código (*RCE*), provocando divulgación de información confidencial en el sistema afectado.

Solución:

Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante, mediante el siguiente enlace:

- https://github.com/auth0/node-jsonwebtoken/releases/tag/v9.0.0

Información adicional:

- https://securityaffairs.com/140596/hacking/jsonwebtoken-library-rce.html
- https://www.bleepingcomputer.com/news/security/auth0-fixes-rce-flaw-in-jsonwebtoken-library-used-by-22-000-projects/
- https://nvd.nist.gov/vuln/detail/CVE-2022-23529
- https://github.com/auth0/node-jsonwebtoken/releases/tag/v9.0.0