BOLETÍN DE ALERTA

Boletín Nro.: 2022-53
Fecha de publicación: 27/12/2022
Tema: Vulnerabilidad de ejecución arbitraria de código en la librería *npm* JSON5

Los productos afectados son:

- JSON5, versiones anteriores a 2.2.2.

Descripción:

Recientemente se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad con *PoC* pública que afecta a la librería *npm* JSON5 de JSON, que permitiría a un atacante realizar ejecución de código arbitrario y provocar denegación de servicio (*DoS*) en el sistema afectado.

La vulnerabilidad identificada como CVE-2022-46175, de severidad "Alta" y con puntuación asignada de 7.1. Esta vulnerabilidad se debe a una falla de seguridad contra ataques del tipo *Prototype Pollution* al agregar o modificar las propiedades de *Object.prototype* en la librería *npm* JSON5. Esto permitiría a un atacante realizar ejecución de código arbitrario en el sistema afectado, provocar denegación de servicio (*DoS*), cross-site scripting (*XSS*), escalamiento de privilegios, entre otros.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría realizar ejecución de código arbitrario en el sistema de forma remota.

Solución:

Recomendamos acceder a la actualización de seguridad correspondiente a través del siguiente enlace:

- https://github.com/json5/json5/releases/tag/v2.2.2

Información adicional:

- https://securityonline.info/cve-2022-46175-json5-prototype-pollution-vulnerability/
- https://nvd.nist.gov/vuln/detail/CVE-2022-46175
- https://github.com/json5/json5/security/advisories/GHSA-9c47-m6qq-7p4h
- https://github.com/opensearch-project/OpenSearch-Dashboards/issues/3148
- https://github.com/json5/json5/releases/tag/v2.2.2