Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA21-00351-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	5 de enero de 2021
Última revisión	5 de enero de 2021

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por la Open.js Foundation sobre una serie de vulnerabilidades que afectan a Node.js.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2020-8287
CVE-2020-8265

Impacto

Estas vulnerabilidades son categorizadas como de riesgo medio. CVE-2020-8287 permite a un atacante remoto realizar un ataque conocido como HRS (por HTTP request smuggling), aprovechando una validación incorrecta de las solicitudes HTTP para introducir cabeceras HTTP arbitrarias. Esto se puede usar para realizar ataques de phishing.

Mientras tanto, CVE-2020-8265 posibilita a un atacante remoto realizar un ataque de denegación de servicio (DoS), gracias a un error de uso de memoria después de ser liberada, en el componente TLSWrap.

Productos Afectados

Node.js, versions de la 10.0.0 a la 15.5.0.

Mitigación

Instalar las actualizaciones del sitio del proveedor.

Enlaces

https://nodejs.org/en/blog/release/v12.20.1/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8287

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8265