| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00326-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de noviembre de 2020 |
| Última revisión | 23 de noviembre de 2020 |

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 obtenida de NodeJS referente a vulnerabilidad que permitiría causar una denegación de servicios a través de peticiones DNS. El presente informe incluye la respectiva medida de mitigación.

## Vulnerabilidad

CVE-2020-8277

# CVE-2020-8277

Una aplicación que haya sido construida con NodeJS y que permita realizar peticiones DNS a un host elegido por el usuario podría causar una denegación de servicios (DoS) al forzar a la aplicación resolver un registro DNS con una gran cantidad de respuestas.

## Productos Afectados

Versiones 12.16.3 y superiores en la línea 12.x.
Versiones 14.13.0 y superiores en la línea 14.x
Todas las versiones de la línea 15.x.

## Mitigación

La vulnerabilidad fue mitigada en las versiones 12.19.1 (LTS), 14.15.1 (LTS) y 15.2.1 (versión actual).

## Enlaces

https://nodejs.org/en/blog/vulnerability/november-2020-security-releases/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8277

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.11.23 16:22:51 -03'00'