Alerta de seguridad informática	9VSA20-00136-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de febrero de 2020
Última revisión	07 de febrero 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 información obtenida de múltiples fuentes, referente a múltiples vulnerabilidades que afectan Node.js, la cuales de ser explotadas, permitirían a un atacante realizar ataques de denegación de servicios, entre otros. Este informe incluye la respectiva mitigación.

Vulnerabilidades

CVE-2019-15604
CVE-2019-15605
CVE-2019-15606

Impacto

CVE-2019-15604

Un atacante remoto podría realizar ataques de tipo denegación de servicios debido a la insuficiente validación de los certificados X509 en X509V3_EXT_print(). El atacante podría entregar un certificado especialmente diseñado para causar el ataque.

CVE-2019-15605

Un atacante podría realizar ataques de tipo contrabando de solicitudes HTTP debido a la insuficiente validación del header Transfer-Encoding. El atacante podría enviar peticiones HTTP especialmente diseñadas para realizar el ataque.

CVE-2019-15606

Un atacante podría manipular los headers HTTP debido a la insuficiente validación del espacio en blanco al final de la petición del header. Un atacante podría enviar peticiones HTTP especialmente diseñada a la aplicación y saltarse ciertas restricciones de seguridad.

Productos Afectados

Para la versión 10, desde la 10.0.0 hasta la 10.18.1.

Para la versión 12, desde la 12.0.0 hasta la 12.14.1.

Para la versión 13, desde la 13.0.0 hasta la 13.7.0.

Mitigación

Para la versión 13, actualizar a la 13.8.0.

Para la versión 12, actualizar a la 12.15.0.

Para la versión 10, actualizar a la 10.19.0.

Enlaces

https://github.com/nodejs/node/blob/master/doc/changelogs/CHANGELOG_V13.md#13.8.0
https://www.cybersecurity-help.cz/vdb/SB2020020615

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15604

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15605

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15606