

Alerta de seguridad cibernética	9VSA20-00225-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de mayo de 2020
Última revisión	26 de mayo 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 afectada a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de jQuery referente a vulnerabilidad que afecta a su biblioteca multiplataforma JavaScript. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2020-7656

CVE-2020-7656

Debido a que la función “load()” falla al reconocer y remover las marcas HTML <script> que contengan un espacio en blanco, por ejemplo, “</script >”, esto permitiría a un atacante remoto realizar ataques XSS (Cross-site Scripting) para el robo de información sensible, engañar usuarios, cambiar la apariencia del sitio, etc.

Nota: Existen formas públicas de explotar esta vulnerabilidad, por lo que se recomienda actualizar a la brevedad.

Productos Afectados

jQuery desde la versión 1.0 hasta la 1.8.3.

Mitigación

Actualizar a jQuery a la versión 1.9.0 o superior.

Enlaces

<https://snyk.io/vuln/SNYK-JS-JQUERY-569619>

<https://github.com/jquery/jquery/blob/9e6393b0bcb52b15313f88141d0bd7dd54227426/src/ajax.js#L203>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7656>