Una vulnerabilidad grave afecta a todas las versiones de la biblioteca Lodash

Autor: I. Stepanenko

Fecha: Thursday 9th of July 2020 06:42:09 PM

Lodash, una biblioteca npm popular utilizada por más de 4 millones de proyectos tan solo en GitHub, se ha visto afectada por una vulnerabilidad de seguridad de alta criticidad, que podría permitir a los hackers comprometer la seguridad de los servicios afectados utilizando la biblioteca y su respectiva base de usuarios.

Lodash es una biblioteca de JavaScript que contiene herramientas para simplificar la programación con cadenas, números, matrices, funciones y objetos, lo que ayuda a los programadores a escribir y mantener su código JavaScript de una forma más eficiente.

Liran Tal, un defensor de desarrolladores en la plataforma de seguridad de código abierto Snyk, publicó hace poco los detalles de prueba de concepto de una vulnerabilidad de seguridad de contaminación de prototipos de alta gravedad que afecta a todas las versiones de Lodash, incluida la última versión 4.17.11.

La vulnerabilidad, asignada como CVE-2019-10744, puede afectar a una gran cantidad de proyectos front-end debido a la popularidad de lodash que se está descargando a una tasa de más de 80 millones de veces por mes.

La contaminación de prototipos es una vulnerabilidad que permite a los atacantes modificar el prototipo de objeto JavaScript de una aplicación web, que es como una variable que se puede utilizar para almacenar múltiples valores basados en una estructura predefinida.

Estas estructuras y valores predeterminados se denominan prototipos que impiden que una aplicación se forme un hash cuando no se establecen valores.

Sin embargo, si un atacante logra inyectar propiedades en el lenguaje JavaScript existente, construye prototipos y manipula estos atributos para sobrescribirlos o contaminarlos, esto podría afectar la forma en que la aplicación procesa los objetos JavaScript por medio de la cadena de prototipos, lo que lleva a un problema de denegación de servicio o ejecución remota de código.

Según Tal, la función *«defaultsDeep»* en la biblioteca de Lodash, podría ser engañada para que agregue o modifique las propiedades de *Object.prototype* utilizando una carga útil del constructor, lo que podría provocar un bloqueo de la aplicación web o alterar su comportamiento, dependiendo del caso de uso afectado.

Cabe mencionar que no es fácil explotar las fallas de la contaminación de un prototipo y requiere un conocimiento profundo de cómo funciona cada aplicación web específica.

EL investigador informó sobre la vulnerabilidad a John Dalton, el encargado del mantenimiento de Lodash, y propuso correcciones que se incluirán en la siguiente versión de la biblioteca.