Se reveló una vulnerabilidad de ejecución remota de código autenticado previamente en dotCMS, un sistema de gestión de contenido de código abierto escrito en Java y «*utilizado por más de 10,000 clientes en más de 70 países de todo el mundo, de marcas Fortune 500 y empresas medianas».*

La vulnerabilidad crítica, rastreada como CVE-2022-26352, proviene de un ataque transversal de directorio al realizar cargas de archivos, lo que permite que un adversario ejecute comandos arbitrarios en el sistema subyacente.

> *«Un atacante puede cargar archivos arbitrarios en el sistema. Al cargar un archivo JSP en el directorio raíz de Tomcat, es posible lograr la ejecución del código, lo que lleva a la ejecución del comando»,* dijo Shubham Shah de Assetnote.

En otras palabras, se puede abusar de la vulnerabilidad de carga de archivos arbitrarios para reemplazar los archivos ya existentes en el sistema con un shell web, que luego se puede utilizar para obtener acceso remoto persistente.

Aunque el exploit hizo posible escribir en archivos JavaScript arbitrarios servidos por la aplicación, los investigadores dijeron que la naturaleza del error era tal que podría convertirse en un arma para obtener la ejecución del comando.

AssetNote dijo que descubrió e informó la falla el 21 de febrero de 2022, luego de lo cual se lanzaron parches en las versiones 22.03, 5.3.8.10 y 21.06.7.

> *«Cuando los archivos se cargan en dotCMS a través de la API de contenido, pero antes de que se conviertan en contenido, dotCMS escribe el archivo en un directorio temporal. En el caso de esta vulnerabilidad, dotCMS no desinfecta el nombre del archivo pasado a través del encabezado de solicitud de varias partes y, por lo tanto, no desinfecta el nombre del archivo temporal»*, dijo la compañía.

> *«En el caso de este exploit, un atacante puede cargar un archivo .jsp especial en el directorio webapp/ROOT de dotCMS que puede permitir la ejecución remota de código»,* agregó.