La Agencia de Ciberseguridad y Seguridad de Infraestructura de EE. UU. (CISA) añadió el martes una vulnerabilidad crítica que afecta al sistema de planificación de recursos empresariales (ERP) de código abierto Apache OFBiz a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV), señalando que existe evidencia de explotación activa.

La vulnerabilidad, identificada como CVE-2024-38856, tiene un puntaje CVSS de 9.8, lo que la clasifica como de gravedad crítica.

> *«Apache OFBiz presenta una vulnerabilidad de autorización incorrecta que podría permitir la ejecución remota de código a través de un payload Groovy en el contexto del proceso de usuario de OFBiz por parte de un atacante no autenticado»,* explicó CISA.

Los detalles de esta vulnerabilidad se hicieron públicos a principios de este mes cuando SonicWall la describió como un bypass de parche para otra falla, CVE-2024-36104, que permite la ejecución remota de código mediante solicitudes especialmente diseñadas.

> *«Una falla en la funcionalidad de vista de sobrecarga expone puntos finales críticos a actores maliciosos no autenticados que utilizan una solicitud diseñada, abriendo la puerta a la ejecución remota de código»*, indicó el investigador de SonicWall, Hasib Vhora.

Este desarrollo surge casi tres semanas después de que CISA incluyera una tercera vulnerabilidad que afecta a Apache OFBiz (CVE-2024-32113) en el catálogo KEV, tras reportes de que había sido explotada para desplegar la botnet Mirai.

Aunque no hay informes públicos sobre cómo se está utilizando CVE-2024-38856, se han publicado exploits de prueba de concepto (PoC).

La explotación activa de dos fallas en Apache OFBiz indica que los atacantes están demostrando un interés considerable en aprovechar vulnerabilidades divulgadas públicamente para comprometer instancias vulnerables con fines maliciosos.

Se recomienda a las organizaciones que actualicen a la versión 18.12.15 para protegerse contra esta amenaza. Se ha ordenado a las agencias de la Rama Ejecutiva Civil Federal (FCEB) que implementen las actualizaciones necesarias antes del 17 de septiembre de 2024.