Los expertos en ciberseguridad han ideado un código de prueba de concepto (PoC) que aprovecha una reciente vulnerabilidad crítica revelada en el sistema de Planificación de Recursos Empresariales (ERP) de código abierto Apache OfBiz para ejecutar una carga útil residente en la memoria.

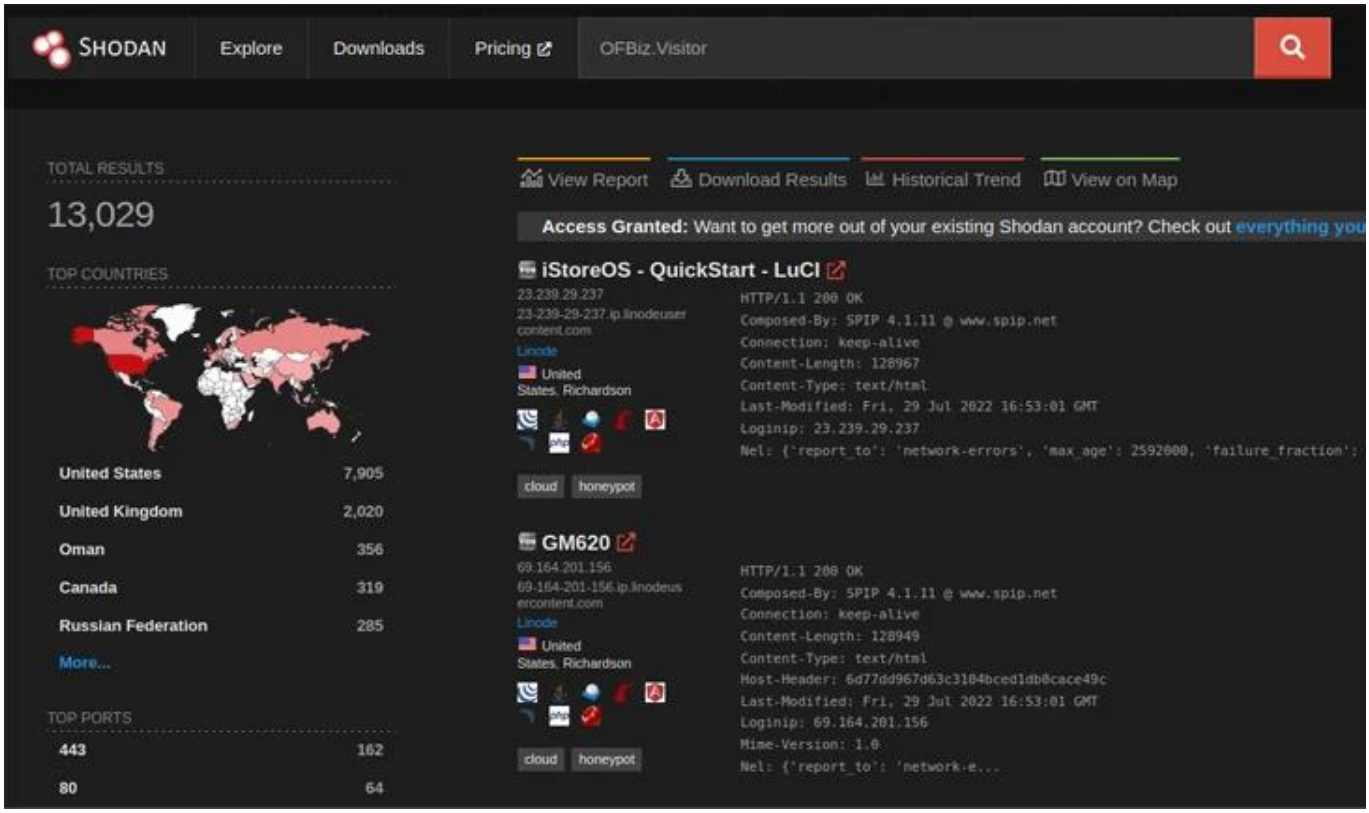
La vulnerabilidad en cuestión es la CVE-2023-51467 (puntuación CVSS: 9.8), una forma de eludir otra debilidad grave en el mismo software (CVE-2023-49070, puntuación CVSS: 9.8) que podría ser utilizado para sortear la autenticación y ejecutar código arbitrario de manera remota.

Aunque fue corregido en la versión 18.12.11 de Apache OFBiz lanzada el mes pasado, se ha observado que actores de amenazas intentan aprovechar la falla, dirigiéndose a instancias vulnerables.

Los últimos hallazgos de VulnCheck muestran que la CVE-2023-51467 puede ser explotada para ejecutar una carga útil directamente desde la memoria, dejando pocas o ninguna evidencia de actividad maliciosa.

Vulnerabilidades de seguridad divulgadas en Apache OFBiz (por ejemplo, CVE-2020-9496) han sido explotadas por actores de amenazas en el pasado, incluidos aquellos asociados con la botnet Sysrv. Otro fallo en el software, con tres años de antigüedad (CVE-2021-29200), ha sido objeto de intentos de explotación desde 29 direcciones IP únicas en los últimos 30 días, según datos de GreyNoise.

Además, Apache OFBiz fue uno de los primeros productos en tener un exploit público para Log4Shell (CVE-2021-44228), lo que indica que sigue siendo de interés tanto para defensores como para atacantes.



La CVE-2023-51467 no es una excepción, con detalles sobre un punto final de ejecución remota de código («/webtools/control/ProgramExport») y un PoC para la ejecución de comandos que aparecen apenas días después de su divulgación pública.

Aunque se han implementado medidas de seguridad (es decir, el sandbox de Groovy) que bloquean cualquier intento de cargar shells web arbitrarios o ejecutar código Java a través del punto final, la naturaleza incompleta del sandbox significa que un atacante podría ejecutar comandos curl y obtener una shell inversa de bash en sistemas Linux.

> *«Para un atacante avanzado, sin embargo, estas cargas útiles no son ideales. Tocan el disco y dependen del comportamiento específico de Linux»,* dijo Jacob Baines, Director de Tecnología de VulnCheck.

El exploit basado en Go desarrollado por VulnCheck es una solución multiplataforma que funciona tanto en Windows como en Linux y elude la lista de denegación al aprovechar las funciones groovy.util.Eval para lanzar una shell inversa Nashorn en memoria como carga útil.

> *«OFBiz no es ampliamente popular, pero ha sido explotado en el pasado. Hay bastante expectación en torno a CVE-2023-51467 pero no hay una carga útil pública y weaponizada, lo que planteó la pregunta de si era posible. Hemos concluido que no solo es posible, sino que podemos lograr una ejecución de código arbitrario en memoria»*, dijo Baines.