La empresa de seguridad de WordPress, Wordfence, dijo el jueves que comenzó a detectar intentos de explotación dirigidos a la vulnerabilidad recientemente revelada en Apache Commons Text, el pasado 18 de octubre de 2022.

A la vulnerabilidad, rastreada como CVE-2022-42889, también conocida como Text4Shell, se le asignó una clasificación de gravedad de 9.8 de 10 en la escala CVSS, y afecta a las versiones 1.5 a la 1.9 de la biblioteca.

También es similar a la vulnerabilidad Log4Shell en el sentido de que el problema radica en la forma en que las sustituciones de cadenas realizadas durante las búsquedas de DNS, secuencias de comandos y URL podrían conducir a la ejecución de código arbitrario en sistemas susceptibles al pasar una entrada que no es de confianza.

> *«El atacante puede enviar una carga útil manipulada de forma remota usando búsquedas de 'script', 'dns' y 'url' para lograr la ejecución remota de código arbitrario»,* dijo el equipo de Zscaler ThreatlabZ.

Una explotación exitosa de la vulnerabilidad puede permitir que un atacante abra una conexión de shell inversa con la aplicación vulnerable simplemente por medio de una carga útil especialmente diseñada, abriendo efectivamente la puerta para ataques de seguimiento.

Aunque el problema se informó originalmente a inicios de marzo de 2022, Apache Software Foundation (ASF) lanzó una versión actualizada del software (1.10.0) el 24 de septiembre, y después emitió un aviso la semana pasada, el 13 de octubre.

> *«Afortunadamente, no todos los usuarios de esta biblioteca se verían afectados por esta vulnerabilidad, a diferencia de Log4j en la vulnerabilidad Log4Shell, que era vulnerable incluso en sus casos de uso más básicos»,* dijo Yaniv Nizry, investigador de Checkmarx.

> *«Apache Commons Text debe usarse de cierta forma para exponer la superficie de ataque y hacer que la vulnerabilidad sea explotable».*

Wordfence también reiteró que la probabilidad de una explotación exitosa tiene un alcance significativamente limitado en comparación con Log4j, con la mayoría de las cargas útiles observadas hasta ahora diseñadas para buscar instalaciones vulnerables.

> *«Un intento exitoso daría como resultado que el sitio web de la víctima realice una consulta de DNS al dominio de escucha controlado por el atacante»,* dijo Ram Gall, investigador de Wordfence.

El investigador agregó que las solicitudes con prefijos de script y URL han sido comparativamente más bajas en volumen.

En todo caso, el desarrollo es otra indicación de los posibles riesgos de seguridad que plantean las dependencias de código abierto de terceros, lo que requiere que las organizaciones evalúen de forma rutinaria su superficie de ataque y establezcan estrategias de administración de parches adecuadas.

Se recomienda a los usuarios que tienen dependencias directas en Apache Commons Text que actualicen a la versión fija para mitigar posibles amenazas. Según Maven Repository, hasta 2593 proyectos usan la biblioteca, aunque Flashpoint dijo que muy pocos de los enumerados usan el método vulnerable.

La vulnerabilidad de Apache Commons Text también sigue a otra debilidad de seguridad crítica que se reveló en la configuración de Apache Commons en julio de 2022 (CVE-2022-33980), lo que podría resultar en la ejecución de código arbitrario por medio de la funcionalidad de interpolación variable.