China suspende acuerdo con Alibaba por no compartir primero con el gobierno los detalles de la vulnerabilidad 0-Day de Log4j

Autor: I. Stepanenko

El regulador de Internet de China, el Ministerio de Industria y Tecnología de la Información (MIIT), suspendió de forma temporal una asociación con Alibaba Cloud, la subsidiaria de computación en la nube del gigante del comercio electrónico Alibaba Group, durante seis meses debido a que no informó de inmediato al gobierno sobre una vulnerabilidad de seguridad crítica que afecta a la biblioteca de registro Log4j, de uso generalizado.

El hecho fue revelado por Reuters y South China Morning Post, citando un informe de 21st Century Business Herald, un diario de noticias de negocios chino.

> «Alibaba Clud no informó inmediatamente las vulnerabilidades en el popular marco de registro de código abierto Apache Log4j2 al regulador de telecomunicaciones de China. En respuesta, MIIT suspendió una asociación cooperativa con la unidad de nube con respecto a las amenazas de ciberseguridad y las plataformas de intercambio de información», dijo Reuters.

Rastreada como CVE-2021-44228, con puntaje CVSS de 10 y nombrada en código Log4Shell o LogJam, la vulnerabilidad crítica permite a los atacantes ejecutar remotamente código arbitrario al obtener una cadena especialmente diseñada registrada por el software.

Log4Shell salió a la luz luego de que Chen Zhaojun, del equipo de seguridad en la nube de Alibaba envió un correo electrónico alertando a la Apache Software Foundation (ASF) el 24 de noviembre sobre la falla, agregando que *«tiene un gran impacto».*

Pero justo cuando se estaba implementando la solución, un actor no identificado compartió los detalles de la vulnerabilidad en una plataforma de blogs china el 8 de diciembre, lo que hizo que el equipo de Apache luchara por lanzar un parche el 10 de diciembre.

Después de la divulgación pública del error, Log4Shell ha sido objetivo de una explotación generalizada por parte de los actores de amenazas para tomar el control de servidores susceptibles, gracias al uso casi omnipresente de la biblioteca, que se puede encontrar en una variedad de servicios para consumidores y empresas, sitios web y aplicaciones, así como en productos de tecnología operativa, que dependen de él para registrar información de seguridad y rendimiento.

En los días siguientes, una mayor investigación sobre Log4j por parte de la comunidad de seguridad cibernética descubrió tres vulnerabilidades más en la herramienta basada en Java, lo que llevó a los encargados del mantenimiento del proyecto a enviar una serie de actualizaciones de seguridad para contener ataques del mundo real que explotan las debilidades.

La compañía de seguridad cibernética Check Point, dijo que ha bloqueado más de 4.3 millones de intentos de explotación hasta el momento, con el 46% de esas intrusiones realizadas por grupos maliciosos conocidos.

«Esta vulnerabilidad puede hacer que el dispositivo sea controlado de forma remota, lo que provocará serios peligros como el robo de información sensible y la interrupción del servicio del dispositivo», dijo anteriormente el MIIT en un comunicado público el 17 de diciembre, agregando que solo se conoció la falla el 9 de diciembre, 15 días después de la divulgación

inicial.

El rechazo del MIIT llega meses después de que el gobierno chino emitiera nuevas regulaciones de divulgación de vulnerabilidades más estrictas que exigen a los proveedores de software y redes afectados por fallas críticas, junto con entidades o personas involucradas en el descubrimiento de vulnerabilidades de seguridad de productos de red, informarlas de primera mano a las autoridades gubernamentales de forma obligatoria dentro de dos días.

En septiembre, el gobierno también siguió con el lanzamiento de *«bases de datos profesionales de seguridad y vulnerabilidad en el ciberespacio»*, para informar sobre vulnerabilidades de seguridad en redes, aplicaciones móviles, sistemas de control industrial, automóviles inteligentes, dispositivos de IoT, entre otros productos de Internet que podrían ser atacados por actores de amenazas.

Después de que el regulador de seguridad de Internet de China eliminara a Alibaba Cloud de su asociación de inteligencia de amenazas cibernéticas durante seis meses, la compañía de computación en la nube dijo este jueves que trabajará para mejorar su gestión de riesgos y cumplimiento, según un nuevo informe del South China Morning Post. Alibaba Cloud también dijo que no comprendía completamente la gravedad de la falla y que no compartió los detalles con el gobierno de forma oportuna.