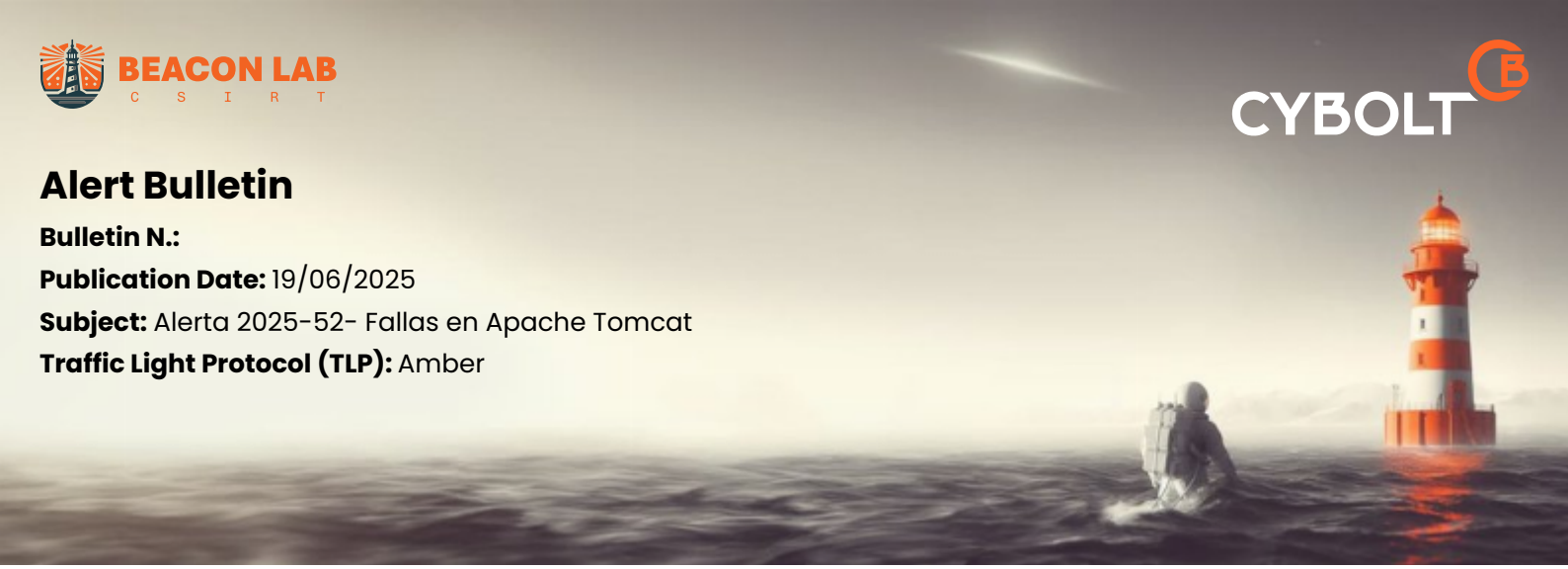

Alert Bulletin

Bulletin N.:
Publication Date: 19/06/2025
Subject: Alerta 2025-52- Fallas en Apache Tomcat
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Apache Tomcat 9.0.0.M1 hasta 9.0.105
- Apache Tomcat 10.1.0-M1 hasta 10.1.41
- Apache Tomcat 11.0.0-M1 hasta 11.0.7

Descripción

La Fundación Apache ha revelado **cuatro vulnerabilidades** que afectan a diversas versiones del servidor Apache Tomcat etiquetadas como: **CVE-2025-48976, CVE-2025-48988, CVE-2025-49124 y CVE-2025-49125**. Estas fallas pueden causar desde denegaciones de servicio (DoS) hasta fallos de seguridad en la instalación y omisión de restricciones de acceso.

A continuación, se describen brevemente:

- **CVE-2025-48976 (7.5) – DoS por encabezados grandes:**

Un atacante puede enviar solicitudes con muchos encabezados grandes para consumir memoria del servidor y hacerlo caer (DoS).
Solución:: ahora se puede limitar el tamaño de encabezado con el parámetro maxPartHeaderSize (por defecto 512 bytes).

- **CVE-2025-48988 (7.5) – DoS por número excesivo de partes:**

El atacante abusa del número de partes en una carga para agotar la memoria compartida y causar una caída del sistema.
Solución:: se ha añadido el parámetro maxPartCount, que limita a 10 partes por defecto.

- **CVE-2025-49124 (8.4) – Riesgo de carga lateral en Windows:**

El instalador usaba icacls.exe sin ruta completa, lo que permitía ejecutar un archivo malicioso con ese nombre.
Riesgo bajo, pero relevante en entornos manipulables.

- **CVE-2025-49125 (7.5) – Omisión de restricciones de seguridad:**

Si una aplicación web usa recursos previos o posteriores montados fuera de la raíz, un atacante puede acceder a ellos saltándose las reglas de seguridad.
Riesgo moderado.

Solución:

Se recomienda **actualizar Apache Tomcat** a la versión más reciente según corresponda:

- **Apache Tomcat 11.0.8 o posterior**

  https://tomcat.apache.org/download-11.cgi

- **Apache Tomcat 10.1.42 o posterior**

  https://tomcat.apache.org/download-10.cgi

- **Apache Tomcat 9.0.106 o posterior**

  https://tomcat.apache.org/download-90.cgi

Información adicional:

- https://securityonline.info/apache-tomcat-patches-4-flaws-dos-privilege-bypass-installer-risks-addressed/
- https://lists.apache.org/thread/0jwb3d3sjyfk5m6xnnj7h9m7ngxz23db