Boletín de alerta

Boletín Nro.: 88
Fecha de publicación: 20/10/2025
Tema: Alerta 2025-88 Vulnerabilidad crítica en Apache Tomcat de ejecución remota de código
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Apache Tomcat versiones
  - **11.0.0-M1 hasta 11.0.2,**
  - **10.1.0-M1 hasta 10.1.34,**
  - **9.0.0-M1 up to 9.0.98.**

Descripción

Recientemente, la Apache Software Foundation reveló la vulnerabilidad **CVE-2025-24813** en sus productos Apache Tomcat, un servidor de servlets Java muy utilizado para aplicaciones web Java. Esta vulnerabilidad permitiría a un atacante poder subir un archivo .session malicioso y luego provocar su deserialización para ejecutar código arbitrario, pero para esto se deben con condiciones específicas.

El problema ocurre cuando el servlet por defecto de Tomcat tiene habilitada la escritura (*writeEnabled*), algo que está **desactivado por defecto**, y el servidor admite solicitudes HTTP de tipo partial PUT (actualización parcial del recurso). Entonces, un atacante puede explotar la equivalencia de ruta para ver archivos sensibles, inyectar contenido o incluso lograr ejecución remota de código a través de un ataque de deserialización.

Para que se logre ejecución de código remoto, además de escritura habilitada en el servlet y soporte partial PUT, se requieren de ciertos parámetros como que la aplicación debe usar la persistencia de sesiones basada en archivos en la ubicación por defecto de Tomcat, y debe existir una biblioteca vulnerable que permita la deserialización maliciosa.

Solución:

La principal solución es actualizar a una versión de Apache Tomcat no vulnerable:

- Para la rama 11.x: actualizar a **11.0.3** o posterior.
- Para la rama 10.1.x: actualizar a **10.1.35** o posterior.

- Para la rama 9.0.x: actualizar a **9.0.99** o posterior.

Si no es posible actualizar de inmediato, se recomienda implementar mitigaciones adicionales:

- Asegurarse de que el servlet por defecto **no tenga habilitada la escritura** (writeEnabled=»false»).
- Deshabilitar o bloquear solicitudes HTTP de tipo partial PUT si no se necesitan.
- Limitar la persistencia de sesiones en archivos, o bien cambiar a otro mecanismo que no dependa de archivos .session.
- Aplicar controles de acceso a nivel de red, como filtros que bloqueen solicitudes PUT hacia directorios públicos.
- Monitorear los logs en busca de solicitudes PUT, de subida de archivos con nombres extraños (por ejemplo archivos .session) o actividad de deserialización sospechosa.

Información adicional:

- https://www.rapid7.com/blog/post/2025/03/19/etr-apache-tomcat-cve-2025-24813-what-you-need-to-know/
- https://nvd.nist.gov/vuln/detail/CVE-2025-24813
- https://www.akamai.com/blog/security-research/march-apache-tomcat-path-equivalence-traffic-detections-mitigations