La empresa informó que detectó un aumento en los intentos de fuerza bruta e inicio de sesión el 5 de junio de 2025, lo cual sugiere que podrían tratarse de acciones deliberadas para *"identificar y acceder a servicios Tomcat expuestos a gran escala".*

Con relación a esto, se identificaron 295 direcciones IP únicas participando en ataques de fuerza bruta contra Tomcat Manager en esa fecha, todas catalogadas como maliciosas. En las últimas 24 horas, se han registrado 188 IP únicas, en su mayoría procedentes de Estados Unidos, Reino Unido, Alemania, Países Bajos y Singapur.

De manera similar, se observaron 298 direcciones IP diferentes intentando iniciar sesión en instancias de Tomcat Manager. De las 246 IP detectadas en las últimas 24 horas, todas fueron clasificadas como maliciosas y provienen de las mismas regiones mencionadas.

Los objetivos de estos ataques incluyen, durante el mismo periodo, a Estados Unidos, Reino Unido, España, Alemania, India y Brasil. GreyNoise señaló que una parte significativa de esta actividad proviene de infraestructura alojada por DigitalOcean (ASN 14061).

> *"Aunque no está vinculada a una vulnerabilidad específica, esta actividad refleja un interés continuo en servicios Tomcat expuestos. Este tipo de actividad amplia y oportunista suele funcionar como una señal temprana de posibles explotaciones futuras",* añadió la empresa.

Como medida preventiva, se recomienda que las organizaciones con interfaces Tomcat Manager accesibles implementen autenticación robusta, restrinjan el acceso adecuadamente y vigilen cualquier indicio de comportamiento sospechoso.

Esta advertencia coincide con la revelación de Bitsight, que informó haber encontrado más de 40,000 cámaras de seguridad accesibles públicamente a través de internet, lo que permitiría a cualquier persona ver las transmisiones en vivo mediante HTTP o el protocolo RTSP (Real-Time Streaming Protocol). Las exposiciones se concentran en países como Estados Unidos, Japón, Austria, Chequia y Corea del Sur.

El sector de las telecomunicaciones representa el 79 % de estas cámaras vulnerables, seguido por tecnología (6 %), medios de comunicación (4,1 %), servicios públicos (2,5 %), educación (2,2 %), servicios empresariales (2,2 %) y administración pública (1,2 %).

Las cámaras se encuentran instaladas en diversos entornos, desde viviendas y oficinas hasta sistemas de transporte público e instalaciones industriales, exponiendo inadvertidamente información sensible que podría ser utilizada para espionaje, acoso o extorsión.

Se aconseja a los usuarios cambiar los nombres de usuario y contraseñas predeterminados, desactivar el acceso remoto si no es necesario (o limitarlo mediante firewalls y VPNs), y mantener el firmware actualizado.

> *"Estas cámaras —diseñadas para brindar seguridad o comodidad— se han convertido, sin querer, en ventanas públicas hacia espacios privados, muchas veces sin que los propietarios lo sepan"*, explicó el investigador de seguridad João Cruz en un informe.
>
> *"Independientemente de los motivos que pueda tener una persona u organización para adquirir estos dispositivos, el hecho de que cualquiera pueda comprarlos, conectarlos y empezar a transmitir con una configuración mínima probablemente explica por qué este sigue siendo un riesgo vigente".*