Se ha revelado una vulnerabilidad crítica de seguridad en la implementación SSH de Erlang/Open Telecom Platform (OTP) que podría permitir a un atacante ejecutar código arbitrario sin necesidad de autenticación, bajo ciertas condiciones.

Esta vulnerabilidad, identificada como CVE-2025-32433, ha recibido la puntuación máxima de 10.0 en el sistema de evaluación de riesgos CVSS, lo que indica su gravedad.

Según investigadores de la Universidad Ruhr de Bochum —Fabian Bäumer, Marcus Brinkmann, Marcel Maehren y Jörg Schwenk—, esta falla permite a un atacante con acceso a la red ejecutar código en un servidor SSH basado en Erlang/OTP sin necesidad de autenticarse previamente.

El origen del problema radica en una gestión incorrecta de los mensajes del protocolo SSH, que permite que un atacante envíe mensajes del protocolo de conexión antes de que se complete la autenticación. Si esta debilidad es aprovechada con éxito, puede derivar en la ejecución de código con los privilegios del servicio SSH.

Lo más preocupante es que, si el daemon SSH se está ejecutando con privilegios de root, el atacante podría tomar el control total del dispositivo. Esto abre la puerta al robo de datos sensibles, interrupción del servicio (DoS) o instalación de malware.

Esta vulnerabilidad afecta a todos los usuarios que utilicen servidores SSH basados en la librería SSH de Erlang/OTP. Se recomienda actualizar a las versiones OTP-27.3.3, OTP-26.2.5.11 o OTP-25.3.2.20. Como solución temporal, es posible bloquear el acceso al servidor SSH vulnerable mediante reglas de firewall adecuadas.

En declaraciones, Mayuresh Dani, gerente de investigación en seguridad en Qualys, calificó esta vulnerabilidad como extremadamente crítica, destacando que podría permitir a un atacante instalar ransomware o robar información sensible.

Dani también señaló que Erlang es comúnmente usado en sistemas de alta disponibilidad por su soporte robusto para procesamiento concurrente, y que la mayoría de los dispositivos de

Cisco y Ericsson utilizan Erlang.

Por lo tanto, cualquier servicio que utilice la librería SSH de Erlang/OTP para acceso remoto —como dispositivos OT, IoT o de computación en el borde— está en riesgo. La forma más efectiva de protegerse es actualizar a una versión corregida del software o a una versión soportada por el proveedor. Si se necesita más tiempo para aplicar las actualizaciones, se recomienda restringir el acceso al puerto SSH únicamente a usuarios autorizados.