Se revelaron un par de vulnerabilidades de seguridad graves en la especificación de la biblioteca de referencia del Módulo de Plataforma Segura (TPM) 2.0, que podrían dar lugar a la divulgación de información a la escalada de privilegios.

Una de las vulnerabilidades, CVE-2023-1017, se refiere a una escritura fuera de los límites, mientras que la otra, CVE-2023-1018, se describe como una lectura fuera de los límites. A la empresa de seguridad cibernética Quarkslab se le atribuye el descubrimiento y la notificación de los problemas en noviembre de 2022.

> *«Estas vulnerabilidades pueden desencadenarse desde aplicaciones en modo usuario al enviar comandos maliciosos a un TPM 2.0 cuyo firmware se basa en una implementación de referencia de TCG afectada»,* dijo Trusted Computing Group (TCG) en un aviso.

Los grandes proveedores de tecnología, las organizaciones que usan computadoras empresariales, servidores, dispositivos IoT y sistemas integrados que incluyen un TPM pueden verse afectados por las vulnerabilidades, dijo Quarkslab, y agregó que *«podrían afectar a miles de millones de dispositivos»*.

TPM es una solución basada en hardware (es decir, un criptoprocesador) que está diseñada para proporcionar funciones criptográficas seguras y mecanismos de seguridad física para resistir los intentos de manipulación.

> *«Las funciones TPM más comunes se usan para medir la integridad del sistema y para la creación y uso de claves. Durante el proceso de inicio de un sistema, el código de inicio que se carga (incluidos el firmware y los componentes del sistema operativo) se puede medir y registrar en el TPM»,* dijo Microsoft en su documentación.

> *«Las medidas de integridad se pueden usar como evidencia de cómo se inició un sistema y para asegurarse de que se usó una clave basada en TPM solo cuando se usó el software correcto para iniciar el sistema».*

El consorcio TCG dijo que las deficiencias son el resultado de la falta de controles de longitud necesarios, lo que genera desbordamientos de búfer que podrían allanar el camino para la divulgación de información local o escalada de privilegios.

Se recomienda a los usuarios que apliquen las actualizaciones publicadas por TCG y otros proveedores para abordar las vulnerabilidades y mitigar los riesgos de la cadena de suministro.

> *«Los usuarios en entornos informáticos de alta seguridad deberían considerar el uso de la atestación remota de TPM para detectar cualquier cambio en los dispositivos y asegurarse de que tu TPM sea a prueba de manipulaciones»,* dijo el Centro de Coordinación CERT (CERT/CC) en una alerta.