Un equipo de investigadores de seguridad cibernética, reveló detalles sobre dos nuevas vulnerabilidades de CPU potencialmente graves, que podrían permitir a los hackers recuperar claves criptográficas protegidas dentro de chips TPM fabricados por STMicroelectronics o Inter TPM basados en firmware.

Trusted Platform Module (TPM), es una solución de seguridad especializada basada en hardware o formware que ha sido diseñada para almacenar y proteger información confidencial de los atacantes, incluso cuando su sistema operativo se ve comprometido.

La tecnología TPM está siendo utilizada ampliamente por millones de computadoras de escritorio, portátiles, servidores, teléfonos inteligentes e incluso, por dispositivos de Internet de las Cosas (IoT), para proteger claves de cifrado, contraseñas y certificados digitales.

Ambas vulnerabilidades, denominadas colectivamente como TPM-Fail, aprovechan un ataque de canal lateral basado en el tiempo para recuperar claves criptográficas.

- CVE-2019-11090: Vulnerabilidades Intel fTPM
- CVE-2019-16863: Chip STMicroelectronics TPM

Según los investigadores, las operaciones de firma de curva elíptica en TPM de varios fabricantes, son vulnerables a problemas de fuga de tiempo, lo que podría conducir a la recuperación de una clave privada al medir el tiempo de ejecución de la operación dentro del dispositivo TPM.

> *«Un adversario privilegiado puede explotar el núcleo del sistema operativo para realizar una medición precisa del tiempo del TPM, y así descubrir y explotar las vulnerabilidades del tiempo en las implementaciones criptográficas que se ejecutan dentro del TPM. Son ataques prácticos. Un adversario local puede recuperar la clave ECDSA de Intel fTPM en 4-20 minutos, dependiendo del nivel de acceso.»*, dicen los investigadores.

- 

Como prueba de concepto, los investigadores probaron y lograron recuperar claves privadas ECDSA y ECSchnorr de 256 bits, mediante la recopilación de datos de temporización de firma con y sin privilegios administrativos.

> *«Además, logramos recuperar las claves ECDSA de un servidor dotado de fTPM que ejecuta StrongSwan VPN en una red ruidosa según lo medido por un cliente».*
>
> *«En este ataque, el cliente remoto recupera la clave de autenticación privada del sector sincronizando solo 45,000 protocolos de autenticación por medio de una conexión de red. El hecho de que un ataque remoto pueda extraer claves de un dispositivo TPM certificado como seguro contra fugas de canal lateral, subraya la necesidad de reevaluar ataques remotos en implementaciones criptográficas».*

Los atacantes pueden usar las claves robadas para falsificar firmas digitales, robar o alterar información encriptada y omitir las características de seguridad del sistema operativo o comprometer las aplicaciones que dependan de la integridad de las claves.

> *«El vulnerable Intel fTPM es utilizado por muchos fabricantes de PC y portátiles, incluidos Lenovo, Dell y HP».*

Además, los investigadores también probaron soluciones TPM fabricadas por Infineon y Nuvoton, y las encontraron vulnerables a problemas de fuga de tiempo de ejecución no constante.

Los investigadores informaron sus hallazgos a Intel y STMicroelectronics en febrero de este

año, las compañías publicaron ayer una actualización de parche para los productos afectados.