Un análisis de imágenes de firmware en dispositivos de Dell, HP y Lenovo reveló la presencia de versiones desactualizadas de la biblioteca criptográfica OpenSSL, lo que subraya un riesgo en la cadena de suministro.

El kit de desarrollo de EFI, también conocido como EDK, es una implementación de código abierto de la interfaz de firmware extensible unificada (UEFI), que funciona como una interfaz entre el sistema operativo y el firmware integrado en el hardware del dispositivo.

El entorno de desarrollo de firmware, que se encuentra en su segunda iteración (EDK II), viene con su propio paquete criptográfico llamado CryptoPkg, que a su vez, hace uso de los servicios del proyecto OpenSSL.

Según la empresa de seguridad de firmware Binarly, se descubrió que la imagen de firmware asociada con los dispositivos empresariales Lenovo Thinkpad, utiliza tres versiones distintas de OpenSSL: 0.9.8zb, 1.0.0a y 1.0.2j, la última de las cuales se lanzó en 2018.

Además, uno de los módulos de firmware llamado InfineonTmpUpdateDxe se basó en OpenSSL versión 0.9.8zb que se envió el 4 de agosto de 2014.

> *«El módulo InfineonTmpUpdateDxe es responsable de actualizar el firmware del Módulo de plataforma segura (TPM) en el chip Infineon«,* dijo Binarly.

> *«Esto indica claramente el problema de la cadena de suministro con dependencias de terceros cuando parece que estas dependencias nunca recibieron una actualización, incluso por problemas críticos de seguridad».*

Dejando a un lado la diversidad de versiones de OpenSSL, algunos de los paquetes de firmware de Lenovo y Dell usaron una versión más antigua (0.9.8l), que salió el 5 de noviembre de 2009. El código de firmware de HP, del mismo modo, usaba una versión de 10

años de la biblioteca (0.9.8w).

El hecho de que el firmware del dispositivo utilice varias versiones de OpenSSL en el mismo paquete binario destaca cómo las dependencias de código de terceros pueden introducir más complejidades en el ecosistema de la cadena de suministro.

Binarly señaló además las debilidades en lo que se llama una Lista de materiales de software (SBOM) que surge como resultado de la integración de módulos binarios compilados (también conocido como código cerrado) en el firmware.

> *«Vemos una necesidad urgente de una capa adicional de validación SBOM cuando se trata de código compilado para validar en el nivel binario, la lista de información de dependencia de terceros que coincide con el SBOM real proporcionado por el proveedor»,* dijo la compañía.

> *«Un enfoque de 'confiar pero verificar' es la mejor forma de lidiar con las fallas de SBOM y reducir los riesgos de la cadena de suministro».*