Un análisis de chats filtrados del grupo de ransomware Conti, reveló a inicios de este año que el sindicato ha estado trabajando en un conjunto de técnicas de ataque de firmware, que podrían ofrecer una ruta para acceder a código privilegiado en dispositivos comprometidos.

> *«El control sobre el firmware otorga a los atacantes poderes prácticamente inigualables tanto para causar daños directamente como para permitir otros objetivos estratégicos a largo plazo»,* dijo la compañía de seguridad de firmware y hardware Eclypsium.

> *«Tal nivel de acceso permitiría a un adversario causar un daño irreparable a un sistema o establecer una persistencia continua que es virtualmente invisible para el sistema operativo».*

Específicamente, esto incluye ataques dirigidos a microcontroladores integrados como Intel Management Engine (ME), un componente privilegiado que forma parte de los conjuntos de chips de procesador de la compañía y que puede eludir completamente el sistema operativo.

Las conversaciones entre los miembros de Conti, que se filtraron luego de que el grupo prometiera su apoyo a Rusia en la invasión de Ucrania por parte de este último, arrojaron luz sobre los intentos del sindicato de explotar vulnerabilidades relacionadas con el firmware ME y la protección contra escritura del BIOS.

Esto implicó encontrar vulnerabilidades y comandos no documentados en la interfaz ME, lograr la ejecución de código en ME para acceder y reescribir la memoria flash SPI, y descartar implantes de nivel de Modo de Administración del Sistema (SMM), que podrían aprovecharse para incluso modificar el kernel.

La investigación finalmente se manifestó en forma de un código de prueba de concepto (PoC) en junio de 2021, que puede obtener la ejecución del código SMM al obtener el control del ME después de obtener acceso inicial al host por medio de vectores tradicionales como phishing, malware, o un compromiso de la cadena de suministro, según los chats filtrados.

> *«Al cambiar el enfoque a Intel ME, así como a los dispositivos de destino en los que el BIOS está protegido contra escritura, los atacantes podrían encontrar fácilmente muchos más dispositivos de destino disponibles»*, dijeron los investigadores.

Además, el control sobre el firmware también podría explotarse para obtener persistencia a largo plazo, evadir soluciones de seguridad y causar daños irreparables en el sistema, lo que permitiría al atacante montar ataques destructivos.

> *«Las filtraciones de Conti expusieron un cambio estratégico que aleja aún más los ataques de firmware de las miradas indiscretas de las herramientas de seguridad tradicionales»*, dijeron los investigadores.

> *«El cambio al firmware ME brinda a los atacantes un grupo mucho más grande de víctimas potenciales para atacar, y una nueva vía para alcanzar el código y los modos de ejecución más privilegiados disponibles en los sistemas modernos».*