Se han revelado hasta 23 nuevas vulnerabilidades de seguridad de alta gravedad en distintas implementaciones de la Interfaz de Firmware Extensible Unificada (UEFI) que utilizan numerosos proveedores, incluyendo a Bull Atos, Fujitsu, HP, Juniper Networks, Lenovo, entre otros.

Las vulnerabilidades residen en el firmware InsydeH2O UEFI de Insyde Software, según la compañía de seguridad de firmware empresarial Binarly, con la mayoría de las anomalías diagnosticadas en el modo de gestión del sistema (SMM).

UEFI es una especificación de software que proporciona una interfaz de programación estándar que conecta el firmware de una computadora a su sistema operativo durante el proceso de arranque. En los sistemas x86, el firmware UEFI suele almacenarse en el chip de memoria flash de la placa base.

> *«Al explotar estas vulnerabilidades, los atacantes pueden instalar con éxito malware que sobrevive a las reinstalaciones del sistema operativo y permite eludir las soluciones de seguridad de punto final (EDR/AV), el arranque seguro y el aislamiento de seguridad basado en virtualización»,* dijeron los investigadores.

La explotación exitosa de las fallas (puntajes CVSS: 7.5 – 8.2) podría permitir que un atacante ejecute código arbitrario con permisos SMM, un modo de ejecución de propósito especial en procesadores basados en x86 que maneja la administración de energía, la configuración del hardware, el monitoreo térmico y otras funciones.

> *«El código SMM se ejecuta en el nivel de privilegio más alto y es invisible para el sistema operativo, lo que lo convierte en un objetivo atractivo para la actividad maliciosa»*, dijo Microsoft en su documentación.

La compañía agregó que el vector de ataque SMM podría ser abusado por un código malicioso para engañar a otro código con mayores privilegios para realizar actividades no autorizadas.

Peor aún, las debilidades también se pueden encadenar para eludir las funciones de seguridad e instalar malware de una forma que sobreviva a las reinstalaciones del sistema operativo y logre una persistencia a largo plazo en los sistemas comprometidos, como se observó en el caso de MoonBounce, mientras se crea sigilosamente un canal de comunicaciones para exfiltrar datos confidenciales.

Insyde lanzó parches de firmware que abordan estas debilidades como parte del proceso de divulgación coordinado. Pero el hecho de que el software se utilice en varias implementaciones de OEM significa que podría tomar una cantidad de tiempo considerable antes de que las correcciones lleguen a los dispositivos afectados.