Investigadores de seguridad cibernética encontraron un *«comportamiento similar a una backdoor»* dentro de los sistemas Gigabyte, que según su investigación, permite que el firmware UEFI de los dispositivos suelten un ejecutable de Windows y recupere actualizaciones en un formato no seguro.

La compañía de seguridad de firmware Eclypsium, dijo que detectó la falla por primera vez en abril de 2023. Desde entonces, Gigabyte reconoció y abordó el problema.

> *«La mayoría del firmware de Gigabyte incluye un ejecutable binario nativo de Windows integrado en el firmware UEFI»,* dijo John Loucaides, vicepresidente senior de estrategia de Eclypsium.

> *«El ejecutable de Windows detectado se coloca en el disco y se ejecuta como parte del proceso de inicio de Windows, similar al ataque de doble agente de LoJack. Este ejecutable después descarga y ejecuta binarios adicionales por medio de métodos inseguros».*

> *«Solo la intención del autor puede distinguir este tipo de vulnerabilidad de una puerta trasera maliciosa»,* agregó Loucaides.

El ejecutable, según Eclypsium, está integrado en el firmware UEFI y el firmware lo escribe en el disco como parte del proceso de arranque del sistema, y posteriormente, se inicia como un servicio de actualización.

La aplicación basada en .NET, por su parte, está configurada para descargar y ejecutar una carga útil desde los servidores de actualización de Gigabyte por medio de HTTP simple, lo que expone el proceso a ataques de adversario en el medio (AitM) por medio de un router comprometido.

Loucaides dijo que el software *«parece haber sido pensado como una aplicación de actualización legítima«*, y dijo que el problema podría afectar *«alrededor de 364 sistemas Gigabyte con una estimación aproximada de 7 millones de dispositivos».*

Debido a que los hackers buscan constantemente formas de pasar desapercibidos y dejar una huella de intrusión mínima, las vulnerabilidades en el mecanismo de actualización de firmware privilegiado podrían allanar el camino para los bootkits e implantes sigilosos de UEFI que pueden subvertir todos los controles de seguridad que se ejecutan en el plano del sistema operativo.

Peor aún es que debido a que el código UEFI reside en la placa base, el malware inyectado en el firmware puede persistir incluso si se borran las unidades y se reinstala el sistema operativo.

Se recomienda a las organizaciones que apliquen las últimas actualizaciones de firmware para minimizar riesgos potenciales. También se recomienda inspeccionar y deshabilitar la función *«Descarga e instalación del centro de aplicaciones»* en la configuración de UEFI/BIOS y establecer una contraseña de BIOS para evitar cambios maliciosos.

> *«Las actualizaciones de firmware tienen una aceptación notoriamente baja entre los usuarios finales. Por lo tanto, es fácil de entender pensando que una aplicación de actualización en el firmware puede ayudar»,* dijo Loucaides.

> *«Sin embargo, la ironía de una aplicación de actualización altamente insegura, respaldada en firmware para descargar y ejecutar de forma automática una carga útil, no se pierde».*