Se ha descubierto una vulnerabilidad de omisión de la función de seguridad en tres cargadores de arranque de interfaz de firmware extensible unificada (UEFI) firmada por terceros, que permite omitir la función UEFI Secure Boot.

> *«Estas vulnerabilidades se pueden explotar montando la partición del sistema EFI y reemplazando el cargador de arranque existente con el vulnerable, o modificando una variable UEFI para cargar el cargador vulnerable en lugar del existente»,* dijo la compañía Eclypsium.

Los siguientes cargadores de arranque específicos del proveedor, que fueron firmados y autenticados por Microsoft, se encontraron vulnerables a la omisión y se parchearon como parte de la actualización Patch Tuesday de la compañía lanzada esta semana:

- Cargador de arranque Eurosoft (CVE-2022-34301)
- Nuevo cargador de arranque de Horizon Data Systems Inc (CVE-2022-34302)
- Cargador de arranque Crypto Pro (CVE-2022-34303)

El arranque seguro es un estándar de seguridad diseñado para evitar que se carguen programas maliciosos cuando una computadora se inicia, y garantiza que solo se inicie el software en el que confía el fabricante de equipos originales (OEM).

> *«Los cargadores de arranque de firmware inician el entorno UEFI y entregan el control a las aplicaciones UEFI escritas por el proveedor de SoC, Microsoft y los OEM. El entorno UEFI inicia el Administrador de arranque de Windows, que determina si se debe iniciar en modo de flasheo de imagen Full Flash Update (FFU) o reinicio del dispositivo, en el sistema operativo de actualización o en el sistema operativo principal»,* dijo Microsoft en su documentación.

En otras palabras, la explotación exitosa de las vulnerabilidades identificadas por Eclypsium podría permitir que un adversario eluda las medidas de seguridad al inicio y ejecute código arbitrario sin firmar durante el proceso de arranque.

Esto puede tener más efectos colaterales, lo que permite que un mal actor obtenga un acceso arraigado y establezca la persistencia en un host de una forma que pueda sobrevivir a las reinstalaciones del sistema operativo y los reemplazos del disco duro, sin mencionar eludir por completo la detección del software de seguridad.

Llamando a CVE-2022-34302 *«mucho más sigiloso»*, Eclypsium dijo que la vulnerabilidad New Horizon Datasys no solo es trivial de explotar en la naturaleza, sino que también puede *«permitir evasiones aún más complejas, como deshabilitar controladores de seguridad».*

Los controladores de seguridad, por ejemplo, pueden incluir mediciones de Trusted Platform Module (TPM) y controles de firma, según los investigadores de Eclypsium, Mickey Shkatov y Jesse Michael.

Cabe mencionar que explotar estas vulnerabilidades requiere que un atacante tenga privilegios de administrador, aunque obtener una escalada de privilegios locales no se considera insuperable debido al hecho de que Microsoft no trata la omisión del Control de Cuentas de Usuario (UAC) como un riesgo de seguridad.

> *«Al igual que BootHole, estas vulnerabilidades resaltan los desafíos de garantizar la integridad de arranque de los dispositivos que dependen de una cadena de suministro compleja de proveedores y códigos que trabajan juntos. Estos problemas resaltan cómo las vulnerabilidades simples en el código de terceros pueden socavar todo el proceso»*, agregaron los investigadores.