Han salido a la luz detalles sobre una vulnerabilidad de seguridad, ya solucionada, que podría permitir evadir el mecanismo de Secure Boot en sistemas con la Interfaz de Firmware Extensible Unificada (UEFI).

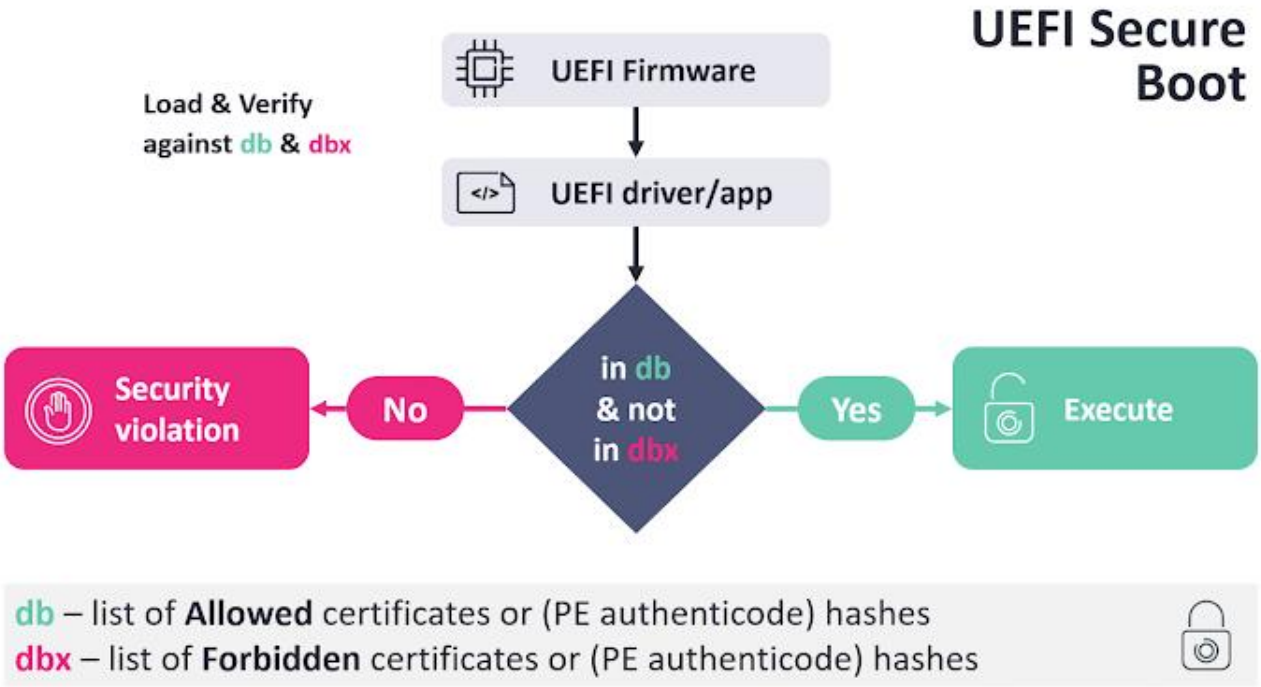
Esta vulnerabilidad, identificada como CVE-2024-7344 y con una puntuación CVSS de 6.7, se encuentra en una aplicación UEFI firmada con el certificado de terceros de Microsoft «Microsoft Corporation UEFI CA 2011», según un reciente informe de ESET.

Si la falla se explota con éxito, podría permitir la ejecución de código no confiable durante el arranque del sistema, lo que posibilitaría a los atacantes instalar bootkits UEFI maliciosos en dispositivos con Secure Boot habilitado, independientemente del sistema operativo que usen.

Secure Boot es un estándar de seguridad que busca impedir que el malware se cargue al iniciar el sistema, asegurándose de que solo se ejecute software aprobado por el fabricante del equipo original (OEM). Este mecanismo utiliza firmas digitales para verificar la autenticidad, el origen y la integridad del código que se ejecuta.

La aplicación UEFI afectada forma parte de varias herramientas de recuperación en tiempo real desarrolladas por diversas compañías, entre ellas Howyar Technologies Inc., Greenware Technologies, Radix Technologies Ltd., SANFONG Inc., Wasay Software Technology Inc., Computer Education System Inc., y Signal Computer GmbH. Los productos vulnerables incluyen:

- Howyar SysReturn: versiones previas a 10.2.023_20240919
- Greenware GreenGuard: versiones anteriores a 10.2.023-20240927
- Radix SmartRecovery: versiones anteriores a 11.2.023-20240927
- Sanfong EZ-back System: versiones previas a 10.3.024-20241127
- WASAY eRecoveryRX: versiones anteriores a 8.4.022-20241127
- CES NeoImpact: versiones previas a 10.1.024-20241127
- SignalComputer HDD King: versiones anteriores a 10.3.021-20241127



> *"El problema se origina por el uso de un cargador PE personalizado en lugar de las funciones estándar y seguras de UEFI, LoadImage y StartImage. Esto permite que la aplicación cargue cualquier binario UEFI, incluso si no está firmado, desde un archivo específicamente diseñado llamado cloak.dat al iniciar el sistema, sin importar el estado de Secure Boot"*, explicó Martin Smolár, investigador de ESET.

Un atacante que aproveche esta vulnerabilidad podría eludir las protecciones de Secure Boot en UEFI y ejecutar código no firmado durante el arranque, antes de que el sistema operativo se inicie, logrando así acceso persistente y encubierto al equipo.

> *"El código que se ejecuta en esta etapa inicial del arranque puede mantenerse en el sistema, incluso cargando extensiones maliciosas del kernel que sobreviven a los reinicios y a la reinstalación del sistema operativo. Además, este tipo de ataque*

> *podría evadir la detección de medidas de seguridad basadas en el sistema operativo, como las soluciones de detección y respuesta de endpoints (EDR)”*, señaló el CERT Coordination Center (CERT/CC).

Un actor malicioso podría ampliar el impacto de este ataque utilizando su propia copia del archivo vulnerable *reloader.efi* en cualquier sistema UEFI que tenga registrado el certificado de terceros de Microsoft. Sin embargo, sería necesario contar con privilegios elevados, como administrador en Windows o root en Linux, para instalar los archivos vulnerables en la partición EFI.

La empresa de ciberseguridad ESET informó este hallazgo al CERT/CC en junio de 2024. Posteriormente, Howyar Technologies y sus socios corrigieron los problemas en los productos afectados. El 14 de enero de 2025, Microsoft revocó los binarios vulnerables como parte de las actualizaciones de seguridad de Patch Tuesday.

Además de aplicar las revocaciones de UEFI, otras medidas de protección incluyen restringir el acceso a los archivos de la partición EFI, personalizar la configuración de Secure Boot y emplear herramientas de atestación remota con módulos de plataforma confiable (TPM).

> *“La creciente cantidad de vulnerabilidades en UEFI descubiertas en los últimos años, y las demoras para parchearlas o revocar binarios inseguros, muestran que incluso una función tan crítica como Secure Boot no es completamente infalible”*, indicó Smolár.

> *“Lo que más nos preocupa de esta vulnerabilidad no es tanto el tiempo que llevó corregirla y revocar el binario, que fue relativamente rápido en comparación con otros casos, sino el hecho de que este no es un caso aislado. Descubrir un binario UEFI firmado y tan inseguro plantea preguntas sobre cuán extendidas están estas prácticas entre los desarrolladores de software UEFI de terceros y cuántos otros cargadores de arranque similares podrían estar ahí fuera».*