Bypass de protección UEFI mediante Windows Recovery Environment

Investigación publicada en CERT/CC VINCE (VU#226679) · 22 de junio de 2026

research UEFI / firmware responsible disclosure

Resumen

Esta investigación documenta un bypass de la protección UEFI a través del Entorno de Recuperación de Windows (WinRE), disponible en cualquier instalación Windows con la configuración por defecto. El comportamiento se descubrió y reprodujo sobre un **HP ZBook Firefly 14 inch G11**, pero la raíz del problema no está en el firmware del fabricante: está en cómo WinRE (un componente de **Microsoft Windows**) interactúa con las políticas de autenticación de arranque externo (*Administrator Authentication Policies*) del firmware UEFI, saltándoselas por completo.
El resultado fue la publicación del **Vulnerability Note VU#226679** en el portal VINCE del **CERT Coordination Center de Carnegie Mellon University**, agradeciéndome el descubrimiento.

¿Qué es UEFI y qué protege la contraseña de administrador?

UEFI (*Unified Extensible Firmware Interface*) es el firmware que reemplazó a la BIOS tradicional y actúa como puente entre el hardware y el sistema operativo durante el arranque. Entre sus funciones de seguridad se encuentra la posibilidad de configurar una **contraseña de administrador UEFI** que, combinada con las **Administrator Authentication Policies**, restringe el acceso al menú de arranque único (F9) y obliga a autenticarse antes de poder arrancar desde dispositivos externos o no autorizados.

El problema: WinRE como vía de escape

El Windows Recovery Environment (WinRE) es un entorno de recuperación incluido por defecto en todas las instalaciones de Windows. Se activa, entre otras formas, manteniendo pulsada la tecla **Shift durante un reinicio**. Una vez dentro, una de sus opciones es **"Usar un dispositivo"**, que permite seleccionar desde qué medio arrancar el equipo.

El problema es que, cuando se usa esta opción, el sistema arranca desde el dispositivo externo seleccionado **sin solicitar la contraseña de administrador UEFI**, aunque esta esté configurada y las políticas de autenticación de arranque externo estén activas.

Técnicamente, esto ocurre porque WinRE utiliza la variable **BootNext** de la NVRAM de UEFI, que permite especificar un destino de arranque único para el siguiente ciclo. Esta variable tiene precedencia sobre el BootOrder habitual y, en muchas implementaciones de firmware, no se somete a las mismas comprobaciones de autenticación que el acceso directo al menú de arranque.

En otras palabras: la contraseña UEFI protege la puerta principal, pero WinRE deja abierta una ventana trasera.

Entorno de prueba y Proof of Concept

Dispositivo: HP ZBook Firefly 14 inch G11

Versión de BIOS: W70 Ver. 01.06.10

Sistema operativo: Windows 11 (configuración por defecto)

WinRE: Habilitado

Contraseña admin UEFI: Habilitada

Restricciones de arranque: Administrator Authentication Policies activas para dispositivos externos

Los pasos para reproducir el comportamiento son los siguientes:

1. Iniciar sesión en Windows con cualquier cuenta de usuario local.
2. Reiniciar el sistema manteniendo pulsada la tecla **Shift** para entrar en WinRE.
3. Seleccionar la opción **"Usar un dispositivo"**.
4. Elegir un medio externo de arranque (por ejemplo, un USB con Kali Linux o cualquier live OS).
5. Observar que el sistema arranca desde el dispositivo externo **sin solicitar la contraseña de administrador UEFI**.

Impacto de seguridad

Un atacante con acceso físico al equipo podría:

- Arrancar un sistema operativo no autorizado desde un medio externo.
- Eludir los controles de seguridad a nivel de sistema operativo y los mecanismos de protección de endpoints.
- Acceder o manipular el almacenamiento local (dependiendo del estado del cifrado de disco).
- Realizar ataques offline: extracción de credenciales, evasión forense o exfiltración de datos.

Este problema es especialmente relevante en entornos empresariales, gubernamentales o de alta seguridad donde la protección UEFI se considera un control de defensa sólido frente a modificaciones no autorizadas del sistema.

Timeline del proceso de divulgación responsable

21 dic 2025	Reporte inicial enviado al equipo de seguridad de **HP (HP PSRT)**.
22 dic 2025	HP asigna el caso al **HP Product Security Response Team** e inicia la evaluación.
27 feb 2026	HP confirma que sigue evaluando la vulnerabilidad.

18 mar 2026	HP responde oficialmente: consideran que el comportamiento no es exclusivo de sus plataformas sino consistente con el diseño actual del ecosistema UEFI/OS, y que requeriría cambios coordinados a nivel de industria. **HP decide no publicar una actualización de firmware.**
20 mar 2026	Reporte enviado al **CERT Coordination Center (Carnegie Mellon University)** a través del portal VINCE.
7 abr 2026	Reporte enviado a **Microsoft Security Response Center (MSRC)**.
10 abr 2026	Seguimiento con Microsoft.
30 abr 2026	Los ingenieros de Microsoft confirman que están revisando el caso.
8 may 2026	Microsoft responde al CERT y cierra el caso por su parte: severidad **Moderada**, clasificado como *Security Feature Bypass*. Consideran que al requerir acceso físico no cumple el umbral para una corrección inmediata, pero han trasladado el informe al equipo responsable del producto para que evalúe una posible solución y tome las medidas necesarias para proteger a los clientes.
22 jun 2026	Publicación del **Vulnerability Note VU#226679** en el portal CERT/CC VINCE de Carnegie Mellon University.
Jul. 2026	Reconocimiento en las **Special Mentions** del Microsoft Researcher Recognition Program (2026), que reconoce a investigadores que han tenido un impacto significativo ayudando a proteger el ecosistema Microsoft.
26 oct. 2026	MITRE asigna el identificador **CVE-2026-116638** a esta vulnerabilidad.

Por qué se reportó primero a HP

El comportamiento se descubrió y reprodujo sobre un **HP ZBook Firefly 14 inch G11**, por lo que el primer reporte fue a HP, que es lo lógico: encontré el problema en un dispositivo suyo. Sin embargo,

tanto HP en su respuesta como el propio CERT/CC durante el proceso de coordinación fueron dejando claro que la raíz del problema no está en el firmware de HP sino en **WinRE, un componente del sistema operativo Windows**. Eso explica por qué el peso de la investigación acabó recayendo en Microsoft como vendor responsable, aunque el detonante fuese un equipo HP.

Respuesta de los vendors

El CERT contactó a múltiples fabricantes de firmware y hardware. El resultado fue el esperado en este tipo de vulnerabilidades de diseño sistémico:

Afectado	GIGABYTE
No afectado	American Megatrends Incorporated (AMI)
No afectado	Insyde Software Corporation
Desconocido	Acer
Desconocido	Amazon
Desconocido	ASUSTeK Computer Inc.
Desconocido	Dell
Desconocido	Extreme Computing Emdoor Rugged
Desconocido	Fujitsu
Desconocido	Gamma Tech Computer Corp.
Desconocido	GETAC Inc.
Desconocido	Google
Desconocido	Hewlett Packard Enterprise
Desconocido	HP Inc.
No afectado	Intel
Desconocido	Lenovo
Desconocido	Microsoft
No afectado	Phoenix Technologies
Desconocido	ReactOS
Desconocido	Star Labs Online Limited
No afectado	Supermicro

Desconocido	Toshiba Corporation
Desconocido	Uniwill

La gran mayoría de vendors contactados por el CERT/CC no respondieron o dejaron su estado sin confirmar. El silencio es en sí mismo una respuesta: nadie quiere asumir la responsabilidad de un problema que atraviesa toda la cadena, del firmware al sistema operativo. GIGABYTE fue el único confirmado como **afectado**, aunque su respuesta también tiró balones fuera, apuntando al ecosistema más amplio en lugar de comprometerse con una corrección concreta. HP, en su comunicación directa conmigo, hizo algo parecido: reconoció que el fallo no es exclusivo de su plataforma y que requeriría cambios coordinados a nivel de industria (honesto, sí, pero también la forma más educada de decir que nadie lo va a arreglar a corto plazo).

Mitigaciones recomendadas

El CERT/CC recoge las siguientes mitigaciones para entornos de alta seguridad:

1. Deshabilitar o restringir WinRE en sistemas donde la funcionalidad de recuperación no sea operativamente necesaria.
2. Requerir autorización administrativa con acceso único y efímero antes de habilitar entornos de recuperación.
3. Habilitar BitLocker con **TPM + PIN** o **TPM + Startup Key** para añadir autenticación adicional en escenarios de pre-arranque.
4. Restringir el uso de medios extraíbles con particiones EFI y cualquier modificación de la NVRAM UEFI, incluyendo las variables BootNext y BootOrder.
5. Desplegar soluciones EDR con capacidades de seguridad pre-arranque y tecnologías de arranque medido (*measured boot*).
6. Implementar controles de seguridad física: bloqueos de dispositivos, almacenamiento seguro y procedimientos de custodia para sistemas de alto valor.

Reflexión final

Cuando Microsoft comunicó la resolución del caso, añadieron una aclaración que me pareció llamativa: *"Microsoft issues CVEs for*

Critical/Important severity cases. As this case is assessed Moderate, no CVE will be issued."

La clasificación como severidad Moderada responde a los criterios establecidos por Microsoft, donde el requisito de acceso físico reduce el nivel de riesgo dentro de su modelo de evaluación. Es una posición coherente con su política. Dicho esto, vale la pena señalar que la contraseña de administrador UEFI existe precisamente para controlar ese acceso físico, por lo que la premisa que reduce la severidad es también la que define el escenario de ataque. Es una tensión propia de vulnerabilidades que operan en la frontera entre firmware y sistema operativo, donde los modelos de amenaza de cada capa no siempre se alinean.

Dicho esto, estoy muy contenta de haber podido aportar mi granito de arena. Esta investigación ha sido especial para mí porque es la primera que sale del ámbito web, que es en lo que me he centrado hasta ahora. Investigar a nivel de firmware me ha abierto una perspectiva completamente nueva y tengo muchas ganas de seguir explorando en esa dirección.

Es cierto que muchos vendors echaron balones fuera apuntando a la especificación UEFI como responsable. Pero que el problema haya quedado documentado públicamente en el CERT/CC ya tiene valor por sí solo, porque obliga a la industria a ser consciente del gap existente entre las garantías que promete la contraseña UEFI y lo que WinRE permite hacer en la práctica.

Quiero agradecer especialmente a **Wade Sparks (VulnCheck)** por sus consejos sobre cómo afrontar este tipo de procesos de divulgación en vulnerabilidades sistémicas donde los vendors tienden a deflectar, y a **Vijay Sarvepalli (VINCE / Carnegie Mellon University)** por su profesionalidad y rigor durante todo el proceso de divulgación responsable.

Para mí, esta investigación tiene un significado especial más allá del resultado técnico. Que mi nombre figure en los reconocimientos del **CERT/CC de Carnegie Mellon University** (uno de los CNAs más prestigiosos del mundo en materia de divulgación de vulnerabilidades) es algo que no me esperaba cuando empecé a investigar esto. Y a eso se suma que esta investigación aparece en

las **Special Mentions** del Microsoft Researcher Recognition Program (2026), que reconoce a investigadores que han tenido un impacto significativo ayudando a proteger el ecosistema Microsoft. Saber que estoy reconocida en dos sitios tan relevantes (Microsoft y el CERT/CC) me llena de orgullo. Es la confirmación de que este trabajo valió la pena.

Referencias

- **CERT/CC Vulnerability Note VU#226679**
- **CVE-2026-116638 — MITRE / CVE.org**
- UEFI Specification, BootNext variable (UEFI Forum)
- **Eclypsium Research Blog** (recomendaciones de mitigación adaptadas por el CERT/CC)

← Anterior
Hacktivismo Italia 2025

Siguiente
Cuando la curiosidad no mata →

Compartir:

© 2026 Beatriz Fresno Naumova — beafn28.es. Todos los derechos reservados.

Política de privacidad · Términos de uso · Política de cookies