Alerta

Técnica

Vulnerabilidades Detectadas en Windows BitLocker

COLCERT AL-20250912-075

TLP:CLEAR

Se ha identificado un conjunto de vulnerabilidades en **BitLocker** (**CVE-2025-54911** y **CVE-2025-54912**) que permiten la elevación de privilegios locales mediante fallos de tipo **use-after-free** los cuales son errores de memoria. Un programa sigue usando un bloque de memoria que ya fue liberado. Esto puede provocar fallos o que un atacante lo aproveche para **ejecutar código malicioso** y **tomar control del sistema.**

Aunque no existen reportes confirmados de explotación activa, **la probabilidad de que actores maliciosos desarrollen exploits funcionales es alta**, dado el atractivo de comprometer sistemas con cifrado de disco. Esto podría derivar en accesos no autorizados a información sensible en entornos corporativos y gubernamentales, con consecuencias legales, operativas y reputacionales.

En un escenario futuro, un ataque exitoso facilitaría el **movimiento lateral** y el **escalamiento en infraestructuras críticas**, reduciendo la efectividad de los controles actuales de seguridad. La principal incertidumbre radica en la velocidad con la que emerjan exploits públicos, lo que obliga a priorizar la aplicación inmediata de parches y medidas de contención dentro de una estrategia preventiva.

Vulnerabilidades identificadas

CVE	PRODUCTO	SCORE CVSS	DESCRIPCIÓN	ACCIONES RECOMENDADAS
CVE-2025-54911	Microsoft Windows 10. Microsoft Windows 11. Microsoft Windows Server.	**7.3 (Alta)**	Falla de tipo use-after-free que permite a un atacante con credenciales locales de bajo privilegio y cierta interacción del usuario **elevar privilegios** hasta nivel SYSTEM.	❑ Aplicar los parches de seguridad de Microsoft (Patch Tuesday, sept. 2025).
CVE-2025-54912	Microsoft Windows 10. Microsoft Windows 11. Microsoft Windows Server.	**7.8 (Alta)**	Falla de tipo use-after-free que también permite **escalamiento de privilegios**, posiblemente con menor necesidad de interacción del usuario, facilitando un control completo del sistema afectado.	❑ Instalar de inmediato el parche oficial de Microsoft. ❑ Implementar medidas de contención en sistemas que no puedan parchearse de inmediato.

NIVEL DE RIESGO

ALTO

¿Cómo se podrían explotar estas vulnerabilidades?

Las vulnerabilidades **CVE-2025-54911 y CVE-2025-54912** son de tipo **"use-after-free"** en BitLocker, lo que permite a un ciberdelincuente manipular la forma en que Windows gestiona la memoria liberada. Esto significa que un programa intenta usar un espacio de memoria que ya ha sido liberado, abriendo una ventana de oportunidad.

Para explotarla, un atacante podría colocar su propio código malicioso en ese espacio de memoria justo después de que se libere. Cuando BitLocker intenta acceder de nuevo a esa memoria, en lugar de encontrar su dato original, ejecuta el código del atacante, lo que podría comprometer la seguridad del sistema.

1. **Acceso local al sistema**: El atacante necesita estar en el equipo (ya sea como usuario con bajos privilegios, un empleado malintencionado (*insider*) o mediante *malware* inicial).
2. **Ejecución de código preparado**: Se crea un programa o archivo que interactúe con BitLocker de forma específica para provocar el error de memoria (use-after-free).
3. **Reutilización de memoria**: Tras liberar un bloque de memoria, el cibercriminal lo reemplaza con datos/control malicioso.
4. **Elevación de privilegios**: Si el exploit tiene éxito, el código malicioso se ejecuta con privilegios de **SYSTEM**, lo que le da control total del equipo (bypasseando las protecciones del cifrado).
5. **Impacto posterior**: Con esos privilegios, se pueden desactivar defensas, instalar puertas traseras, acceder a información sensible o moverse lateralmente en la red.

Diferencia clave entre ambas vulnerabilidades

- En **CVE-2025-54911** se requiere interacción del usuario (ejemplo: abrir o ejecutar algo que el atacante prepare).
- En **CVE-2025-54912** el ataque sería más directo, sin depender tanto de esa interacción, lo que la hace más peligrosa.

IMPACTO PARA COLOMBIA Y LA REGIÓN

- **Sectores afectados**: Abarcan en general los sectores estratégicos del país, especialmente aquellos reconocidos como infraestructuras críticas cibernéticas (gobierno, financiero, TIC, salud, educación, transporte).
- **Riesgo alto:** Las vulnerabilidades permiten elevar privilegios a nivel SYSTEM lo que da control profundo del sistema. El cifrado de disco (BitLocker) se usa comúnmente para proteger datos críticos y asegurar integridad/confidencialidad.
- **Posibles consecuencias**: Exfiltración de datos sensibles, daño reputacional para entidades afectadas, pérdida de confianza ciudadana, interrupción operativa de servicios esenciales.
- **Implicaciones en seguridad digital**: Necesidad de establecer procedimientos de gestión de vulnerabilidades. Destinar inversión en herramientas y servicios de monitoreo, detección temprana de anomalías, capacitación técnica.

Son vulnerabilidades que por sí solas no permiten acceso remoto, pero sí convierten un acceso local limitado en un control total del sistema, lo que aumenta mucho el riesgo si se combinan con otras técnicas (como phishing o exploits de ejecución remota).

Aunque no hay reportes públicos de explotación masiva aún, la probabilidad de desarrollo de exploit real es relevante.

Técnicas MITRE ATT&CK asociadas

TÉCNICA	CÓDIGO	DESCRIPCIÓN
Explotación para escalamiento de privilegios	T1068	Los adversarios explotan vulnerabilidades en software, drivers o servicios del sistema operativo para obtener privilegios más altos en un sistema. En este caso, las fallas en BitLocker permiten pasar de un usuario de bajos privilegios a SYSTEM.
Vaciamiento de Procesos	T1055.012	Adversarios pueden inyectar código malicioso en procesos suspendidos y vaciados para evadir defensas basadas en procesos y posiblemente elevar privilegios, ejecutando código arbitrario en el espacio de direcciones de un proceso vivo separado.

Mitigaciones MITRE

MITIGACIÓN	CÓDIGO	RELEVANCIA
Actualización de software	M1051	Aplicar parches de Microsoft corrige directamente las vulnerabilidades de use-after-free en BitLocker, evitando que puedan ser explotadas.
Restricción de permisos de usuario	M1026	Limitar los privilegios de las cuentas locales reduce la probabilidad de que un atacante con bajos privilegios pueda aprovechar estas vulnerabilidades para escalar a SYSTEM.
Gestión de privilegios de cuentas	M1018	Controlar y monitorear las cuentas con privilegios administrativos previene que un exploit exitoso se combine con credenciales privilegiadas para ampliar el impacto.
Monitoreo y análisis de comportamiento de aplicaciones	M1040	Soluciones EDR/antivirus con detección de anomalías pueden identificar intentos de explotación en memoria o de inyección en procesos legítimos como parte de la cadena de ataque.

Soluciones y mitigaciones disponibles

- **Aplicar los parches oficiales de Microsoft**: Ambas vulnerabilidades ya fueron corregidas en el Patch Tuesday de septiembre de 2025. Instalar estas actualizaciones en todos los equipos con Windows (10, 11 y versiones de servidor que usen BitLocker). Verificar con inventarios de activos qué máquinas aún no han recibido el parche. (Tener en cuenta el fin del soporte de Windows 10 en octubre)

- **Mantener actualizado Windows Update y WSUS**: Asegurar que los servidores de actualización corporativos distribuyan correctamente los parches.

- **Restringir privilegios**: Reducir cuentas con acceso administrativo local. Usar el principio de menor privilegio para limitar las posibilidades de explotación inicial.

- **Segmentar la red:** Para minimizar movimiento lateral en caso de compromiso. Implementar EDR/antivirus con detección de comportamientos anómalos de escalamiento de privilegios.

- **Reforzar el control de acceso físico y local**: Como el ataque requiere acceso local, reforzar políticas contra el uso indebido de equipos (usuarios internos, dispositivos no autorizados).

- **Implementar procedimientos:** De gestión de vulnerabilidades, que permitan realizar validación y aplicación de actualizaciones de seguridad.

Fuentes

- **Cybersecurity News, 9 septiembre 2025, 11 septiembre 2025, Windows BitLocker Vulnerability: Elevation of Privilege via Use-After-Free (CVE-2025-54911 & CVE-2025-54912), Fuente especializada en ciberseguridad.**
  https://cybersecuritynews.com/windows-bitlocker-vulnerability/

- **Microsoft Security Response Center (MSRC), 9 septiembre 2025, 11 septiembre 2025, CVE-2025-54911 | BitLocker Elevation of Privilege Vulnerability, Fuente oficial del fabricante.**
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-54911

- **Microsoft Security Response Center (MSRC), 9 septiembre 2025, 11 septiembre 2025, CVE-2025-54912 | BitLocker Elevation of Privilege Vulnerability, Fuente oficial del fabricante.**
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-54912

NIVEL DE RIESGO

ALTO

COLCERT