Incidente ID:	0034
Fecha del reporte:	26/09/2025
Entidad:	Entidades del ecosistema digital
Título:	Vulnerabilidades críticas de BitLocker
Herramienta de detección	N/A
Activo involucrado:	BitLocker en Microsoft Windows 10, Microsoft Windows 11 y Microsoft Windows Server.
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Crítico

Objetivo:

Informar a las entidades del Ecosistema Digital sobre las vulnerabilidades críticas descubiertas en BitLocker Microsoft Office (CVE-2025-54911 y CVE-2025-54912), que permiten la elevación de privilegios locales mediante errores use-after-free. El objetivo es promover la aplicación inmediata de los parches de seguridad liberados por Microsoft en septiembre de 2025 y reducir el riesgo de explotación.

Riesgo:

Si no se aplican los parches de seguridad, las vulnerabilidades permitirán que un atacante con acceso local y credenciales de bajo privilegio ejecute código malicioso para obtener control a nivel SYSTEM, comprometiendo la confidencialidad, integridad y disponibilidad de la información protegida con BitLocker.

Actualmente no existen reportes confirmados de explotación activa, la probabilidad de desarrollo de exploits es alta dado al valor de comprometer sistemas con cifrado de disco.

Detalle de la fase 2 – Aplicaciones Afectadas

- Inicio: Nueve (9) de septiembre de 2025 (ciclo de actualizaciones de Microsoft)
- Aplicaciones / Clientes afectados:
- Microsoft Windows 10 .
- Microsoft Windows 11.
- Microsoft Windows server.

Excluidos:

- A la fecha, no se cuenta con información oficial sobre aplicaciones, versiones o entornos excluidos de estas vulnerabilidades.

ámbitos no impactados: Dispositivos que no cuenten con Windows instalado

- Usuarios y/o colaboradores que no trabajen con Sistemas Operativos de Windows

Recomendaciones de actualización:

- Aplicar los parches oficiales de Microsoft publicados para las vulnerabilidades CVE-2025-54911 y CVE-2025-54912 en los equipos con sistema operativo Windows 10, Windows 11 y Windows Server que utilicen BitLocker.

- Mantener actualizado Windows Update y WSUS, verificando que los servidores corporativos distribuyan correctamente los parches.

- Restringir privilegios de cuentas locales, aplicando el principio de menor privilegio.

- Implementar segmentación de red para minimizar el movimiento lateral en caso de compromiso.
- Implementar soluciones EDR/antivirus con detección de comportamientos anómalos asociados a escalamiento de privilegios.
- Establecer procedimientos internos de gestión de vulnerabilidades para validar y aplicar actualizaciones de seguridad.
- Identificar máquinas que aún no hayan recibido el parche, considerando el fin de soporte de Windows 10 en octubre 2025 para planificar su migración.

Pasos para la actualización:

- Identificar todos los equipos con Windows 10, Windows 11 y Windows Server que utilicen BitLocker.
- Descargar e instalar los parches oficiales de Microsoft liberados en el Patch Tuesday de septiembre 2025.
- Validar con inventarios de activos qué máquinas aún no han recibido la actualización.
- Verificar que los servidores corporativos de actualización (Windows Update y WSUS) estén distribuyendo correctamente los parches.
- Confirmar que las actualizaciones se aplicaron exitosamente en los equipos.

Fuentes:

- https://www.colcert.gov.co/800/w3-article-405789.html

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.