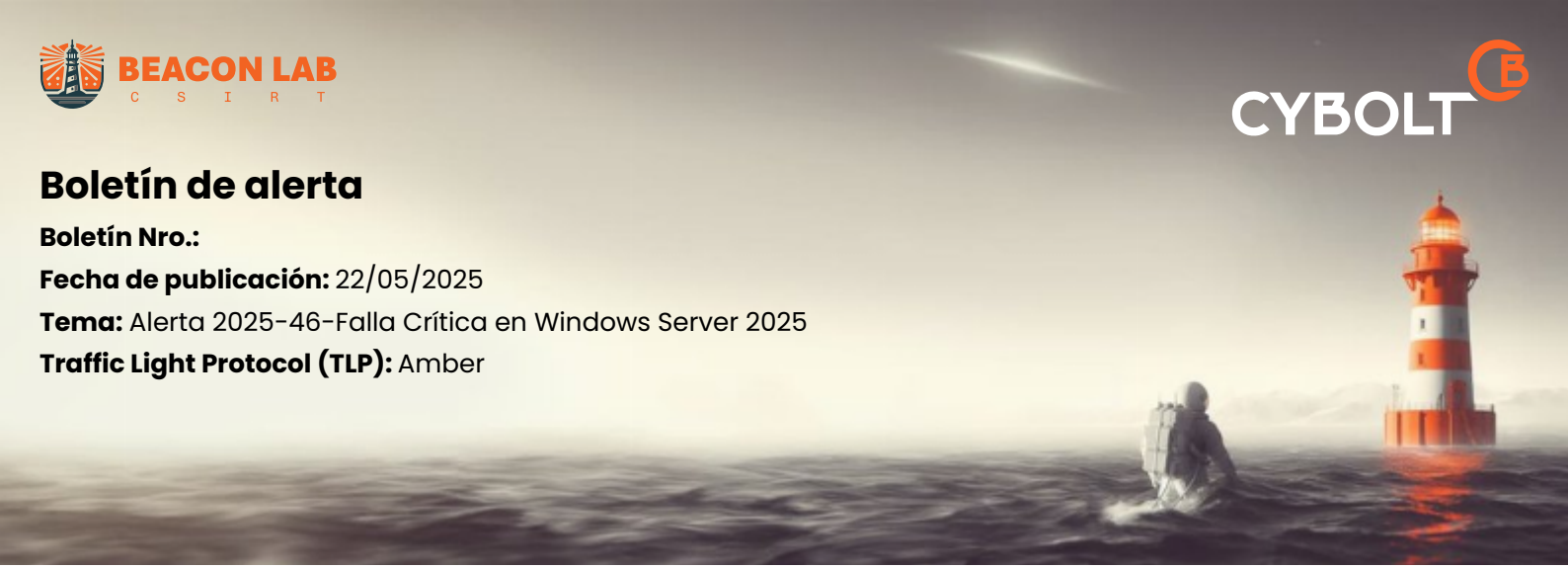

# Boletín de alerta

**Boletín Nro.:**
**Fecha de publicación:** 22/05/2025
**Tema:** Alerta 2025-46-Falla Crítica en Windows Server 2025
**Traffic Light Protocol (TLP):** Amber

## Producto(s) afectado(s):

- Sistema operativo: Microsoft Windows Server 2025
- Componente vulnerable: Active Directory – Mecanismo de autenticación Kerberos / dMSA (Delegated Managed Service Accounts)

## Descripción

Se ha identificado una vulnerabilidad crítica de **escalada de privilegios** en **Windows Server 2025**, relacionada con la nueva función de **Cuentas de Servicio Administradas Delegadas (dMSA)**. Esta falla, descubierta por el investigador Yuval Gordon de Akamai, permite a un atacante con privilegios limitados en Active Directory suplantar la identidad de **cualquier cuenta**, incluyendo administradores de dominio. El ataque, llamado **BadSuccessor**, **funciona por defecto**, **no requiere el uso activo de dMSA** en el entorno y **es explotable mediante un módulo público de Metasploit**. Microsoft ha reconocido la falla, pero **aún no ha publicado un parche oficial**.

Las **dMSA** son un nuevo tipo de cuenta de servicio introducida en Windows Server 2025. Están diseñadas para facilitar la migración de cuentas de servicio no administradas (como cuentas de usuario estándar usadas como servicios) hacia una solución más segura y administrada. Las dMSA heredan configuraciones y permisos de cuentas antiguas mediante un atributo de AD llamado msDS-ManagedAccountPrecededByLink.

Esta característica, pensada para facilitar migraciones, se convierte en el centro de la vulnerabilidad.

El problema radica en que, durante la migración a una dMSA, **el KDC (Centro de Distribución de Claves)** copia automáticamente los privilegios y claves de la cuenta "reemplazada" a la nueva dMSA, **basándose únicamente en un vínculo de atributo** (msDS-ManagedAccountPrecededByLink). Este atributo **puede ser modificado por cualquier usuario que tenga permisos de creación de objetos en una Unidad Organizativa (OU)**.

Esto significa que **un atacante con permisos menores**, como "Crear objetos secundarios" en una OU, puede crear una dMSA y vincularla a **cualquier cuenta del dominio**, incluyendo un administrador de

dominio. Una vez hecho esto, al autenticarse con la nueva dMSA, el sistema le otorgará todos los privilegios de la cuenta original, incluyendo los **tickets de Kerberos (TGT)** y, en algunos casos, **las claves criptográficas de la cuenta suplantada**.

Este ataque no requiere acceso privilegiado ni herramientas especiales, solo el uso de cmdlets estándar como New-ADServiceAccount o herramientas como **Rubeus**, que ahora soporta autenticación con dMSA. Es decir, con solo dos cambios de atributos en AD, un atacante puede comprometer por completo un dominio.

# Solución:

### Detección

Se recomienda a las organizaciones implementar los siguientes controles de monitoreo:

- **Auditoría de creación de objetos dMSA (Evento 5137):** Configure una SACL en el dominio para registrar la creación de objetos del tipo msDS-DelegatedManagedServiceAccount. Preste atención a cuentas que normalmente no deberían estar creando cuentas de servicio.
- **Monitoreo de modificaciones al atributo msDS-ManagedAccountPrecededByLink (Evento 5136):** Este cambio es clave para el ataque. Cualquier modificación debe ser considerada altamente sospechosa.
- **Detección de autenticaciones de dMSA (Evento 2946):** Cuando una dMSA se autentica, el controlador de dominio genera este evento. Si se observa un aumento inesperado o autenticaciones de dMSA poco comunes, debe investigarse.
- **Revisión de permisos en OUs:** Identifique usuarios o grupos que tengan permisos excesivos en OUs, especialmente aquellos que permiten la creación de objetos. En muchos entornos estos permisos se delegan por conveniencia, sin considerar el impacto en seguridad.

### Mitigación recomendada (mientras no haya parche)

Hasta que Microsoft libere un parche oficial, se recomienda lo siguiente:

1. **Auditar los permisos en todas las Unidades Organizativas (OU):** Identifique todos los usuarios o grupos que tengan la capacidad de crear objetos dMSA. Esto puede hacerse con scripts de PowerShell disponibles públicamente (como el publicado por Akamai).

   https://github.com/akamai/BadSuccessor

2. **Restringir la creación de dMSA a administradores de confianza:** Asegúrese de que solo cuentas de administración autorizadas puedan crear dMSAs. Elimine estos permisos de cualquier otra cuenta o grupo.
3. **Supervisar cambios en atributos sensibles:** Especialmente el atributo msDS-ManagedAccountPrecededByLink, ya que su modificación es la base del ataque BadSuccessor.
4. **Implementar alertas de eventos clave (5136, 5137, 2946):** Integre estos eventos en su SIEM para facilitar la detección en tiempo real.

5. **Capacitar al personal de administración de AD:** Asegúrese de que los equipos de infraestructura comprendan los riesgos asociados con permisos excesivos o mal configurados en Active Directory.

## Información adicional:

- https://www.akamai.com/blog/security-research/abusing-dmsa-for-privilege-escalation-in-active-directory
- https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/delegated-managed-service-accounts/delegated-managed-service-accounts-overview