Boletín de alerta

Boletín Nro.: 76
Fecha de publicación: 22/09/2025
Tema: Alerta 2025-76 Vulnerabilidad crítica en Azure Entra ID
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- **Azure Entra ID** (antes Azure Active Directory)

Descripción

El pasado julio, Dirk-jan Mollema, investigador de seguridad de Outsider Security, descubrió y reportó al Centro de Respuestas de Seguridad de Microsoft (MSRC) una **vulnerabilidad crítica** que radica en un fallo en el mecanismo de validación de tokens dentro de Azure Entra ID, la cual **permitía acceso total a recursos, creación de cuentas, elevación de privilegios y manipulación de identidades** en el tenant víctima. Esta vulnerabilidad **CVE-2025-55241** fue categorizada con un puntaje **CVSS de 10.0**, reflejando su facilidad de explotación y el impacto total sobre confidencialidad, integridad y disponibilidad.

El servicio emite “Actor tokens”, un tipo especial de credencial que permite a una aplicación o servicio actuar en nombre de un usuario. Estos tokens deberían estar restringidos al **tenant de origen**, sin embargo, el API legado **Azure AD Graph** no validaba correctamente el campo tid (tenant ID) cuando recibía un Actor token.

Esto significaba que un atacante podía:

1. Crear o comprometer un tenant bajo su control.
2. Solicitar un Actor token válido desde dicho tenant.
3. Reutilizar ese token contra el API de otro tenant víctima.
4. Hacerse pasar por cualquier usuario del tenant destino, incluyendo cuentas con privilegios de **Global Administrator**.

El impacto se agrava porque:

- Los **Actor tokens** no estaban sujetos a **políticas de acceso condicional** ni requerían MFA, lo que permitía evadir controles adicionales de autenticación.
- El uso de estos tokens generaba registros limitados en los logs de auditoría, reduciendo la visibilidad de los equipos de seguridad.

- La vulnerabilidad permitía acceso total a recursos, creación de cuentas, elevación de privilegios y manipulación de identidades en el tenant víctima.

Mitigación y solución:

Microsoft ya desplegó mitigaciones de forma global a mediados de julio de 2025:

- Se corrigió la lógica de validación del tenant ID en la aceptación de Actor tokens dentro de Azure AD Graph.
- Se bloquearon los escenarios en los que un token de un tenant podía ser reutilizado en otro tenant.
- Se aceleró la deshabilitación definitiva de Azure AD Graph API, promoviendo la migración total a Microsoft Graph API, que sí implementa controles modernos de validación.

Recomendaciones para administradores:

1. **Confirmar que su tenant ya recibió la actualización** automática desplegada por Microsoft.
2. **Migrar urgentemente de Azure AD Graph a Microsoft Graph**, dado que el API legado quedará fuera de soporte y representa un riesgo estructural.
3. **Auditar cuentas y roles privilegiados**, buscando accesos inusuales, creación de aplicaciones o delegaciones sospechosas.
4. **Revisar logs y alertas en Microsoft Entra ID Protection** para detectar intentos de explotación.
5. **Aplicar el principio de privilegio mínimo** y revisar asignaciones de “Global Admin”, reduciendo la superficie de impacto.

Información adicional:

- Microsoft Patches Critical Entra ID Flaw Enabling Global Admin Impersonation Across Tenants
- Microsoft soluciona grave vulnerabilidad en Entra ID que permitía suplantar cualquier identidad – Una Al Día
- Critical Microsoft’s Entra ID Vulnerability Allows Attackers to Gain Complete Administrative Control