e-dea NETWORKS | CYBER SECURITY

BOLETÍN
INFORMATIVO

14 – Mayo -2026

Vulnerabilidad en Microsoft

CVE-2026-40379
CVSS 9,3 Critico

Detalles

La vulnerabilidad expone información confidencial en Azure Entra ID, lo que permite a un atacante suplantar identidades en la red. La brecha posibilita que un atacante no autorizado se haga pasar por usuarios o servicios legítimos, obteniendo potencialmente acceso no autorizado a recursos protegidos. La vulnerabilidad se clasifica como CWE-200, lo que indica una falla de exposición de información que puede aprovecharse para eludir la autenticación.

Riesgo

La puntuación EPSS no está disponible, pero la ausencia de una lista KEV no reduce la probabilidad de explotación. Se infiere que el vector de ataque se basa en la red, lo que requiere que un atacante pueda enviar solicitudes manipuladas al punto final ESTS para obtener tokens falsificados u otra información de identificación. Dada la alta gravedad y el potencial de suplantación de identidad, el riesgo para la confidencialidad, la integridad y la disponibilidad es significativo.

Productos Afectados

El servicio Microsoft Enterprise Security Token Service (ESTS) se ve afectado. No se proporciona información específica sobre la versión en los datos disponibles, por lo que todas las implementaciones de ESTS con la funcionalidad expuesta corren riesgo.

Recomendaciones

- Aplique la actualización de seguridad publicada por Microsoft para el Servicio de tokens de seguridad empresarial de Microsoft.
- Restrinja el acceso a la red de los puntos finales de ESTS mediante cortafuegos o segmentación de subredes, de modo que solo los sistemas de confianza puedan acceder al servicio.
- Habilite y supervise los registros de auditoría de los flujos de autenticación de ESTS para detectar la emisión sospechosa de tokens o los intentos de suplantación de identidad.

Fuernte: OpenCVBE