Boletín de alerta

Boletín Nro.:
Fecha de publicación: 16/07/2026
Tema: Alerta 2026-71 Vulnerabilidad 0-day en AnyDesk
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- AnyDesk para Windows
- AnyDesk para Linux
- AnyDesk para macOS

Descripción

Se ha divulgado información sobre la vulnerabilidad **CVE-2026-15682 (CVSS 5.5)**, la cual afecta a **AnyDesk** , una de las plataformas de acceso remoto más utilizadas en entornos empresariales.

De acuerdo con el registro oficial del CVE, la vulnerabilidad permite que un **atacante local** provoque una condición de **denegación de servicio (DoS)** en instalaciones vulnerables de AnyDesk. La explotación puede ocasionar la interrupción del servicio o el cierre inesperado de la aplicación, afectando la disponibilidad de las sesiones remotas.

Aunque distintas publicaciones en redes y foros han descrito esta vulnerabilidad como un «**0-day**«, **al momento de este boletín no existe evidencia pública ni confirmación oficial de que CVE-2026-15682 haya sido explotada activamente en ataques reales** ni de que haya sido incorporada al catálogo de vulnerabilidades explotadas (KEV) de CISA. La información públicamente disponible describe una vulnerabilidad de disponibilidad con impacto local, sin reportes oficiales de explotación *in the wild*.

El riesgo es mayor en organizaciones donde AnyDesk constituye un componente crítico para la administración remota de infraestructura, especialmente si existen usuarios locales con capacidad de ejecutar la aplicación.

Solución

Se recomienda a los administradores realizar las siguientes acciones:

- Actualizar AnyDesk a la versión más reciente publicada por el fabricante.
- Verificar que todos los clientes y servidores ejecuten versiones soportadas.

- Restringir el acceso local a usuarios autorizados únicamente.
- Aplicar el principio de mínimo privilegio en estaciones de trabajo y servidores.

Información adicional:

- CVE Record – CVE-2026-15682 CVE.org
- AnyDesk Security Advisories