

Boletín de alerta

Boletín Nro.: 111

Fecha de publicación: 30/09/2026

Tema: Alerta 2026-111 Vulnerabilidades severas en TeamViewer Full Client y Host

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Producto	Sistemas operativos	Versión corregida
TeamViewer Full Client	Windows, Linux y macOS	15.82 o posterior
TeamViewer Host	Windows, Linux y macOS	15.82 o posterior
Servicios relacionados de TeamViewer	Según versión y plataforma	Aplicar actualización de seguridad equivalente de la rama soportada

TeamViewer informó que las correcciones están disponibles en **TeamViewer Clients 15.82** y en releases de mantenimiento/legacy que continúan bajo soporte.

Descripción

Se han publicado cinco vulnerabilidades de severidad alta que afectan productos TeamViewer: **Full Client** y **Host**. La falla de mayor impacto, **CVE-2026-92370 con un score CVSS 8.8**, es un bypass de control de acceso de sesiones remotas que podría permitir a un atacante realizar acciones no autorizadas y alcanzar ejecución remota de código (**RCE**) en sistemas afectados.

A continuación se listan las vulnerabilidades:

- **CVE-2026-92370 — bypass de control de acceso a sesiones remotas**

CVE-2026-92370 se debe a una debilidad de control de acceso en TeamViewer Full Client y Host para Windows, Linux y macOS. Un atacante remoto podría aprovechar el defecto para ejecutar acciones no autorizadas dentro de una sesión de TeamViewer, lo que puede derivar en ejecución remota de código en el sistema objetivo.

Dado que TeamViewer se utiliza para administración remota, soporte técnico, acceso a endpoints y operación de infraestructura, un bypass de autorización representa un riesgo elevado: el software suele operar con acceso a sistemas corporativos y puede estar permitido a través de firewalls, herramientas de seguridad o controles de acceso remoto.

- **CVE-2026-19743, CVE-2026-92368, CVE-2026-92369 y CVE-2026-92371 — ejecución local y escalación de privilegios**

Las cuatro vulnerabilidades restantes requieren condiciones de explotación local, pero pueden permitir a un usuario o proceso con acceso al sistema incrementar sus privilegios o ejecutar código con el contexto de otro usuario. Los impactos reportados incluyen ejecución de código con los privilegios de la sesión actual y escalación a **NT AUTHORITY \ SYSTEM** en Windows o **root** en sistemas Linux/macOS.

Estas fallas son relevantes en escenarios posteriores a un acceso inicial: un atacante que comprometa una estación de trabajo con privilegios bajos podría abusar de los componentes vulnerables de TeamViewer para ampliar sus privilegios, establecer persistencia y dificultar la detección o remediación.

TeamViewer recomienda actualizar de inmediato a la versión **15.82** o a la actualización equivalente para ramas de mantenimiento y versiones legacy soportadas. La empresa indicó que, al momento de la divulgación, no tenía conocimiento de exploits públicos ni de explotación activa en entornos reales.

Solución

El proveedor recomienda actualizar todos los clientes y hosts a **TeamViewer 15.82 o posterior**, o instalar la actualización equivalente disponible para las ramas de mantenimiento y legacy soportadas.

Guía oficial para actualizar TeamViewer

<https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/update/update-teamviewer/>

Descarga oficial de TeamViewer para Windows

<https://www.teamviewer.com/en/download/portal/windows/>

Información adicional:

- <https://www.bleepingcomputer.com/news/security/teamviewer-urges-users-to-patch-severe-flaws-as-soon-as-possible/>
- <https://www.teamviewer.com/en/resources/trust-center/security-bulletins/tv-2026-1010/>
- <https://www.teamviewer.com/en/resources/trust-center/security-bulletins/>