

Sicherheitslücken in TeamViewer Fernwartungssoftware

Bewertung der Bedrohungslage, CVSS-Klassifizierung und Handlungsempfehlungen für IT-Administratoren

Dringlichkeit: Hoch (CVSSv3 Score 8.8) – Unverzügliches Handeln erforderlich

TeamViewer hat Sicherheitsupdates für fünf Schwachstellen herausgegeben. Die gravierendste Sicherheitslücke erlaubt das Umgehen von Zugriffskontrollen. Administratoren sollten die bereitgestellten Versionen zeitnah auf allen Clients und Hosts ausrollen.

1. Sachliche Einordnung und Faktenlage

Die im Raum stehenden Warnungen und der dringliche Handlungsaufruf an IT-Administratoren sind fachlich vollkommen berechtigt und spiegeln den tatsächlichen Gefährdungsgrad wider. Fernwartungswerkzeuge genießen auf Endgeräten naturgemäß höchste Systemprivilegien und durchdringen Netzwerk- und Firewall-Schranken. Sicherheitsmängel in diesen Kernkomponenten stellen daher ein primäres Ziel für böswillige Akteure dar.

Kennung / Bulletin	CVSS-Score / Risiko	Beschreibung & Auswirkung
CVE-2026-92370	8.8 (Hoch)	Improper Access Control / Permission Bypass im Session-Start für Full Client & Host (Windows, macOS, Linux).
CVE-2026-19743	7.8 (Hoch)	Lokale Rechteausweitung (Privilege Escalation) über fehlerhafte Zugriffsprüfung im lokalen IPC-Dienst.
CVE-2026-92368	7.5 (Hoch)	Heap-basierter Pufferüberlauf bei der Verarbeitung von .tvs-Sitzungsaufzeichnungsdateien.

2. Technische Risikobewertung

- Knapp an 'Kritisch' vorbei:** Mit einem CVSSv3-Score von 8.8 verfehlt die schwerwiegendste Schwachstelle (CVE-2026-92370) die formale Einstufung als 'kritisch' (ab 9.0) nur haarscharf. Die praktische Relevanz ist vergleichbar hoch, da keine Interaktion administrativer Nutzer erforderlich ist.
- Privilege Escalation:** Schadsoftware oder lokale Angreifer mit eingeschränkten Nutzerrechten können über Schwachstellen im Hintergrunddienst (IPC) ihre Rechte auf SYSTEM (Windows) bzw. root (Linux/macOS) ausweiten. Ein kompromittiertes Standard-Benutzerkonto reicht damit zur vollständigen Übernahme des Endgeräts aus.

- **Plattformübergreifende Betroffenheit:** Die Schwachstellen beschränken sich nicht auf ein spezifisches Betriebssystem, sondern betreffen standardmäßig alle weit verbreiteten Plattformen: Windows, macOS und Linux.

3. Konkrete Maßnahmen und Handlungsempfehlungen

- **Sofortige Softwareaktualisierung:** Aktualisierung aller Instanzen von TeamViewer Full Client, Host und Custom-Modulen auf mindestens Version 15.82 bzw. die gepatchten Versionen der LTS-/Legacy-Zweige (z. B. 15.64.8, 14.7.48855).
- **Restriktionen für Sitzungsdateien:** Benutzer sensibilisieren und technische Filter implementieren, um das Ausführen von extern zugesandten .tvs-Sitzungsaufzeichnungen bis zur vollständigen Aktualisierung zu unterbinden.
- **Tenant- und Zugriffskontrollen auditieren:** Überprüfung und Durchsetzung von Conditional-Access-Regeln sowie exklusiven Allowlists (Zulassungslisten) für TeamViewer-IDs in der Management Console, um Sitzungsaufbauten von unautorisierten Dritten netzwerkseitig zu blockieren.

4. Quellen und Verweise

- *TeamViewer Security Bulletin TV-2026-1010 (CVE-2026-92370, CVE-2026-19743, CVE-2026-92368 u. a.)*
- *SecurityOnline / BleepingComputer Berichterstattung (September/Oktober 2026: 'TeamViewer Fixes Five High-Severity Flaws in Full Client and Host')*
- *National Vulnerability Database (NVD) & Common Vulnerability Scoring System (CVSS v3.1)*

Dokument erstellt zur internen Lagebewertung und Dokumentation von Patch-Management-Maßnahmen.