

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



High-Severity Vulnerability in TeamViewer Clients
Tracking #:432316805
Date:29-01-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability has been identified in TeamViewer Clients for Windows, including TeamViewer Remote and TeamViewer Tensor.

TECHNICAL DETAILS:

A high-severity vulnerability (CVE-2025-0065) has been identified in TeamViewer Clients for Windows, including TeamViewer Remote and TeamViewer Tensor.

Vulnerability Overview:

- CVE ID: CVE-2025-0065
- CVSS Score: 7.8 (High)
- Vulnerability Type: CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')
- Affected Products:
 - TeamViewer Full Client (Windows) versions < 15.62, < 14.7.48799, < 13.2.36226, < 12.0.259319, < 11.0.259318
 - TeamViewer Host (Windows) versions < 15.62, < 14.7.48799, < 13.2.36226, < 12.0.259319, < 11.0.259318
- Exploitation Requirement: Local unprivileged access to the Windows system.
- Exploitation Status: No evidence of active exploitation in the wild.

Fixed Version:

- 15.62 or the latest version available

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update all affected TeamViewer Clients and Hosts to fixed or the latest available version.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://www.teamviewer.com/en-us/resources/trust-center/security-bulletins/tv-2025-1001/?>