NCA-25.311026 – National CERT Advisory

NCA-25.311026 : NATIONAL CERT ADVISORY - Potential Remote Code Execution Through Remote-Control Sessions

TeamViewer has disclosed a high-severity vulnerability, tracked as **CVE-2026-111585**, affecting its remote-control clients. The vulnerability stems from an integer overflow in the processing of remote-control screen data and may result in a denial of service or, depending on the platform, potentially enable arbitrary code execution with the privileges of the viewer process.

The vulnerability affects TeamViewer clients prior to version 15.83 across Windows, Linux and macOS, with additional legacy versions identified in the vendor's security bulletin. Exploitation requires a user to establish a remote-control session with an attacker-controlled or compromised host.

Organizations using TeamViewer for remote access, technical support or system administration are encouraged to review their deployments, update affected installations and assess whether existing remote-access controls adequately address the associated risks.

Document Summary

Item	Details
Vulnerability	CVE-2026-111585
Affected software	TeamViewer remote-control clients
Severity	High
CVSS score	8.8
Vulnerability type	Integer overflow
Attack vector	Malicious data processed during a remote-control session
User interaction	Establishment of a remote-control session is required
Potential impact	Denial of service or potential remote code execution
Recommended action	Update to a fixed version and review remote-access security controls
Official reference	TeamViewer Security Bulletin TV-2026-1011

Vulnerability Overview

The vulnerability arises from an integer overflow in the component responsible for processing remote-control screen data. Under certain conditions, a malicious remote host may supply data that triggers the flaw, potentially causing a crash or memory corruption.

Depending on the platform and circumstances, successful exploitation may allow arbitrary code execution with the privileges of the affected viewer process.

Platform / Product	Vulnerable Versions	Fixed / Safe Release
TeamViewer Full Client (Windows, macOS, Linux)	Versions prior to **15.83**	**15.83** or higher
TeamViewer Portable (Windows)	Versions prior to **15.83**	**15.83** or higher
TeamViewer Remote Control App (Android)	Versions prior to fixed release	**15.83** or higher
Legacy Branch 14.x	Older 14.x releases	**14.7.48868**
Legacy Branch 13.x	Older 13.x releases	**13.2.36231**

The vulnerability is particularly relevant to environments where TeamViewer is used to connect to external or otherwise untrusted systems. However, exploitation is not automatic: the vendor indicates that a remote-control session with an attacker-controlled or compromised host is required.

Affected Products and Versions

According to TeamViewer's security bulletin, affected products include:

- TeamViewer Full Client for Windows, Linux and macOS versions prior to 15.83.
- TeamViewer Portable for Windows versions prior to 15.83.
- TeamViewer Remote Control App for Android versions prior to the fixed release identified by the vendor.
- Certain legacy and maintenance versions, including older 15.x, 14.x and 13.x releases, as specified in the official bulletin.

Fixed release: TeamViewer 15.83 or the latest version available for the relevant product and platform.

Organizations using legacy operating systems or older TeamViewer releases may wish to consult the vendor's bulletin for the appropriate fixed version rather than assuming that the standard upgrade path applies.

Potential Impact

Depending on the circumstances, successful exploitation may result in:

- **Service disruption:** The affected TeamViewer client may crash or become unavailable.
- **Potential code execution:** An attacker may be able to execute code with the privileges of the affected viewer process.
- **Endpoint compromise:** Successful code execution may affect the confidentiality, integrity or availability of the endpoint.

- **Operational disruption:** Systems used for remote support, administration or business operations may be affected.
- **Follow-on security risks:** If an endpoint is compromised, the consequences may extend to information or resources accessible to the affected process or user.

The actual impact depends on the platform, process privileges, system configuration and circumstances of exploitation.

Recommended Security Measures

Organizations may consider the following measures to reduce exposure:

- **Update TeamViewer:** Upgrade affected installations to version 15.83 or the latest applicable fixed release.
- **Review deployments:** Identify TeamViewer installations across organizational endpoints, servers and remote-support environments, including portable and legacy versions.
- **Restrict remote access:** Consider limiting remote-control sessions to approved users, trusted partners and authorised devices.
- **Verify connection requests:** Encourage users to verify the identity and legitimacy of the remote party before accepting a session.
- **Review access privileges:** Use standard user privileges where operationally feasible and limit administrative access to situations where it is necessary.
- **Review unattended access:** Assess whether unattended access is required and review associated account permissions and authentication controls.
- **Monitor remote sessions:** Where supported, retain and review relevant connection records, authentication events and endpoint security alerts.
- **Assess legacy systems:** Where an affected version cannot be upgraded immediately, consider restricting its use or network exposure until an appropriate remediation path is available.

These measures may help reduce risk but should complement, rather than replace, the relevant software update.

Monitoring and Detection

Organizations may wish to review available security telemetry for:

- Unexpected TeamViewer client crashes or repeated process restarts.
- Unusual remote-control sessions or connections inconsistent with normal operational activity.
- Endpoint security alerts associated with TeamViewer processes.
- Unexpected child processes or other suspicious activity originating from the TeamViewer client.

- Unusual authentication events or remote-access activity outside approved support arrangements.

Relevant TeamViewer connection records, authentication logs, EDR alerts and endpoint logs may be preserved in accordance with organizational retention policies to support investigation and historical exposure assessment.

These observations are not conclusive evidence of exploitation and should be assessed alongside other available indicators.

Response to Suspected Compromise

Where credible indicators suggest that a TeamViewer-enabled endpoint may have been compromised, organizations may consider:

1. Assessing the affected device, installed TeamViewer version and relevant remote-session history.
2. Restricting or disabling remote access where warranted by the circumstances.
3. Preserving relevant connection logs, endpoint telemetry and security alerts.
4. Investigating suspicious process activity and any unexpected changes to the affected system.
5. Applying the relevant security update and reviewing associated remote-access controls.
6. Considering specialist incident-response assistance if code execution or broader endpoint compromise is suspected.

Immediate Action & Mitigation Matrix

Priority	Stage	Recommended Action	Responsible Team
P1	**Patching**	Upgrade all TeamViewer endpoints to version **15.83** or above.	SysAdmin / Endpoint Management
P2	**Access Control**	Restrict incoming/outgoing remote connections to approved IP lists or domain accounts.	Network / Security Operations
P3	**Workaround**	Block untrusted outbound remote connections if immediate patching isn't possible.	Firewall / SOC Team
P4	**Monitoring**	Audit logs for unexpected TeamViewer process crashes (TeamViewer.exe) or unauthorized sessions.	Threat Intelligence / SIEM Team

References

1. **TeamViewer Security Bulletin TV-2026-1011:** Security Update for Vulnerabilities in TeamViewer Clients. Official TeamViewer Security Bulletin

2. **Canadian Centre for Cyber Security:** TeamViewer Security Advisory (AV26-1093). Canadian Centre for Cyber Security Advisory

Action Summary

Organizations are encouraged to:

- Identify affected TeamViewer installations and assess their exposure.
- Upgrade to the applicable fixed release.
- Review remote-access permissions and connection practices.
- Monitor relevant remote-session and endpoint security logs.
- Investigate credible indicators of compromise and preserve relevant evidence.

Call to Action

The reported vulnerability highlights the importance of maintaining updated remote-access software and applying appropriate safeguards to remote-control sessions. Organizations are encouraged to review their TeamViewer deployments and consider proportionate mitigation measures based on their operational requirements and risk exposure.

For other advisories, please visit the NCERT website: NCERT Advisories

National Cyber Emergency Response Team (NCERT)
Government of Pakistan
Pak Secretariat, L Block, Islamabad
Telephone: +92-51-9203422
Email: info@pkcert.gov.pk
Website: www.pkcert.gov.pk