مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Active Exploitation of TrueConf Vulnerability

Tracking #:432318729

Date:06-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical zero-day vulnerability in the TrueConf Client, tracked as CVE-2026-3502, is actively exploited in targeted cyberattacks against various entities.

TECHNICAL DETAILS:

A critical zero-day vulnerability in the TrueConf Client, tracked as CVE-2026-3502, is actively exploited in targeted cyberattacks against various entities. The vulnerability allows attackers to abuse the software's update mechanism to deliver malicious payloads. The campaign, dubbed Operation TrueChaos, leverages compromised on-premises servers to distribute malware across trusted networks, resulting in large-scale compromise.

Vulnerability Details

- **CVE ID:** CVE-2026-3502
- **CVSS Score:** 7.8 (High)
- **CWE Classification:** CWE-494 (Download of Code Without Integrity Check)
- **Affected Component:** TrueConf Client Update Mechanism
- **Vulnerability Type:** Improper validation of update authenticity and integrity
- **Fixed Version**: TrueConf version 8.5.3 or later

Technical Description

The TrueConf client automatically checks for updates from a central server. However:

- No cryptographic signature verification is enforced
- No integrity validation (e.g., hash verification) is performed
- The client blindly trusts update packages from the server

This enables attackers to:

- Replace legitimate updates with malicious binaries
- Execute arbitrary code during the update process
- Gain user-level or elevated privileges depending on execution context

Attack Campaign: Operation TrueChaos

Overview

Researchers identified a coordinated attack campaign targeting government infrastructure, attributed with moderate confidence to a Chinese-nexus threat actor.

Attack Chain

- Compromise of central TrueConf server within a government IT environment
- Replacement of legitimate client update with weaponized package
- Automatic distribution of malicious update to all connected endpoints
- Execution of malicious payload via trusted update mechanism

Indicators of Compromise:

trueconf_windows_update.exe – Malicious TrueConf client update 22e32bcf113326e366ac480b077067cf
iscsiexe.dll – Loader 9b435ad985b733b64a6d5f39080f4ae0

7z-x64.dll – Havoc implant 248a4d7d4c48478dcbeade8f7dba80b3
43.134.90[.]60 – Havoc C2
43.134.52[.]221 – Havoc C2
47.237.15[.]197 – Havoc C2

RECOMMENDATIONS:

- Immediate Actions
  - Upgrade to TrueConf version 8.5.3 or later immediately
  - Validate integrity of all update packages
  - Isolate affected systems if compromise is suspected
- Scan endpoints for listed IOCs
- Monitor for:
  - DLL side-loading activity
  - Suspicious process execution chains
  - Outbound connections to known C2 IPs

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://nvd.nist.gov/vuln/detail/CVE-2026-3502