Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

TrueConf Zero-Day Abused in Operation TrueChaos to Weaponize Software Updates

Date of Publication	Admiralty Code	TA Number
April 07, 2026	A1	TA2026091

Summary

First Seen: Early 2026
Affected Products: TrueConf Client for Windows
Malware: Havoc C2 framework
Campaign: Operation TrueChaos
Impact: A high-severity flaw in the TrueConf Windows client (CVE-2026-3502) has been actively exploited as a zero-day in Operation TrueChaos, a campaign targeting government entities in Southeast Asia by turning a trusted update mechanism into an attack vector. Due to the absence of integrity checks, attackers were able to hijack the update process on a compromised on-premises server, delivering a trojanized installer that silently deployed a DLL side-loading chain and established access via the Havoc C2 framework. The intrusion quickly progressed with reconnaissance, payload staging, and privilege escalation using living-off-the-land techniques, highlighting how a simple lack of update validation can enable full-scale compromise. The issue has been patched in version 8.5.3, making immediate upgrades and threat hunting critical for affected organizations.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-3502	TrueConf Client Download of Code Without Integrity Check Vulnerability	TrueConf Client	✓	✓	✓

Vulnerability Details

#1

A high-severity security flaw in the TrueConf client video conferencing software has been exploited in the wild as a zero-day as part of a campaign targeting government entities in Southeast Asia, dubbed Operation TrueChaos. Tracked as CVE-2026-3502, the issue affects TrueConf Client for Windows versions 8.1.0 through 8.5.2. The vulnerability stems from the application's built-in update mechanism, which checks an on-premises server for newer versions and prompts users to download and execute updates directly from a server-hosted path.

#2

The core weakness lies in the complete lack of integrity and authenticity verification during this update process. The client does not validate digital signatures, hashes, or any form of trust indicators for the downloaded package. This oversight allows attackers who have compromised the on-premises TrueConf Server or can manipulate the update delivery channel to replace legitimate updates with malicious payloads. The client then executes the tampered file without raising any meaningful warning, effectively turning a trusted update channel into an attack vector.

#3

In the observed in-the-wild exploitation, the attacker had already compromised a government-operated TrueConf on-premises server that served as the video conferencing platform for dozens of government entities across a Southeast Asian country. They weaponized the update mechanism by delivering a trojanized installer that performed a legitimate version upgrade while covertly dropping a benign PowerISO executable alongside a malicious DLL. This DLL was executed via side-loading, enabling initial access through the Havoc command-and-control framework. Follow-on activity included reconnaissance using system utilities, payload retrieval via FTP, environment variable manipulation, and privilege escalation through a UAC bypass leveraging the iscsicpl.exe LOLBIN technique. The overlap in tactics and infrastructure points, with moderate confidence, points to a Chinese-linked threat actor behind the campaign.

#4

TrueConf has remediated the flaw in version 8.5.3, released in March 2026, by introducing stronger validation controls in the update workflow. Organizations using affected versions should prioritize immediate patching and conduct thorough investigations for signs of compromise, particularly focusing on anomalous update behavior, suspicious file placements, and indicators of persistence tied to this attack chain.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-3502	TrueConf Client for Windows (versions 8.1.0 through 8.5.2)	cpe:2.3:a:trueconf:trueconf_client:*:*:*:*:*:*:windows:*:*	CWE-494

Recommendations

Upgrade TrueConf Client Immediately: All organizations running TrueConf Client for Windows must upgrade to version 8.5.3 or later without delay. This version includes the vendor's fix for CVE-2026-3502, which introduces proper integrity validation in the software update mechanism.

Audit TrueConf Server Integrity: Organizations operating on-premises TrueConf Servers should conduct an immediate forensic review of the server to determine whether the update package hosted at the server's ClientInstFiles directory has been tampered with. Specifically, verify that the trueconf_client.exe file in C:\Program Files\TrueConf Server\ClientInstFiles\ is digitally signed by TrueConf and matches the expected hash for the current version. Any unsigned or unexpected executables should be treated as indicators of compromise.

Implement Network Segmentation and Monitoring: Organizations should ensure that TrueConf servers are isolated within network segments with strict access controls, limiting which systems can communicate with the server and monitoring all traffic for anomalies. Enhanced logging should be enabled on TrueConf servers and endpoints to detect unauthorized file modifications, abnormal update behavior, and suspicious outbound connections.

Validate Software Update Mechanisms Across the Enterprise: This incident highlights the broader risk of implicit trust in internal software update channels. Organizations should review all enterprise applications that use on-premises update servers and assess whether those update mechanisms include proper code-signing verification, certificate pinning, and integrity checks. Consider implementing application allowlisting policies that restrict execution of unauthorized binaries, even those delivered through otherwise trusted channels.

Vulnerability Management: Integrate CVE-2026-3502 into existing vulnerability management workflows with the highest remediation priority. Maintain an up-to-date inventory of all TrueConf Client installations across the environment, including both centrally managed deployments and individual user installations. Subscribe to TrueConf's security advisories and CISA KEV catalog updates to ensure timely awareness of future disclosures affecting this and similar enterprise collaboration platforms.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Execution	T1204: User Execution	T1204.002: Malicious File
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
Privilege Escalation	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
Defense Evasion	T1574: Hijack Execution Flow	T1574.001: DLL
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
Discovery	T1057: Process Discovery	
Command and Control	T1071: Application Layer Protocol	
	T1219: Remote Access Software	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	22e32bcf113326e366ac480b077067cf, 9b435ad985b733b64a6d5f39080f4ae0, 248a4d7d4c48478dcbeade8f7dba80b3
IPv4	43[.]134[.]90[.]60, 43[.]134[.]52[.]221, 47[.]237[.]15[.]197

Patch Link

https://trueconf.com/downloads/windows.html

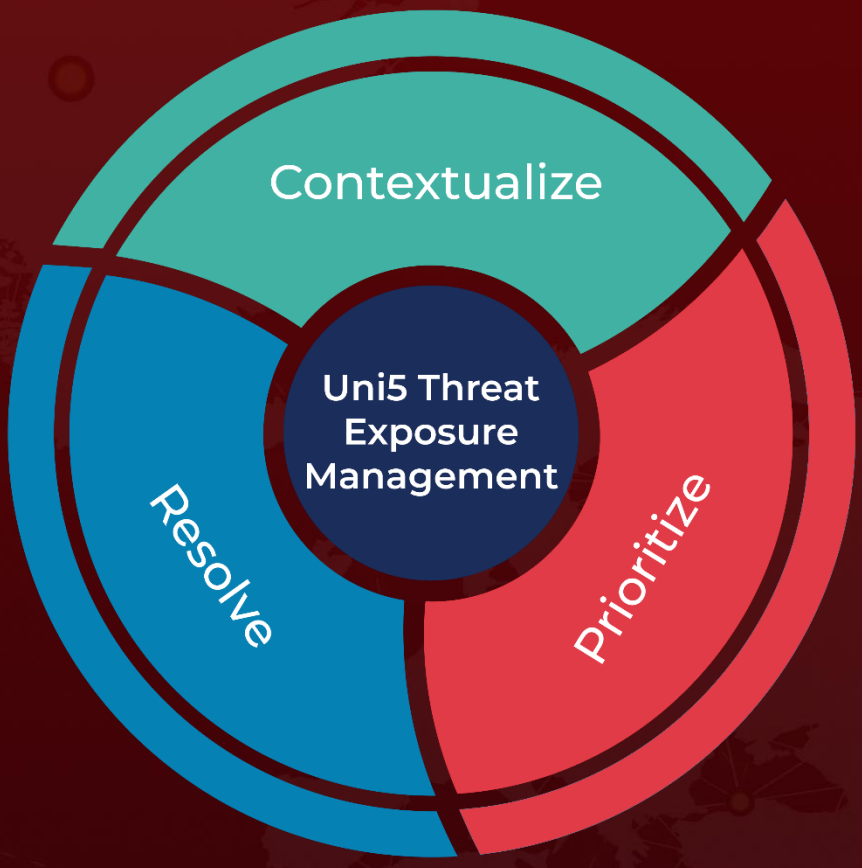
References

https://research.checkpoint.com/2026/operation-truechaos-0-day-exploitation-against-southeast-asian-government-targets/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 07, 2026 • 7:30 AM

More at www.hivepro.com