GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

24 August 2026

Advisory 194: CVE-2026-72530_TrueConf Server Sandbox Escape Vulnerability

Release Date: 19th August 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-72530 is a critical-severity sandbox escape vulnerability in TrueConf Server, an on-premise video conferencing and unified communications platform. It carries a CVSS Base Score of 9.0 and is caused by a code injection flaw (CWE-94) reachable over TCP port 4307, which is open by default on TrueConf Server installations.
This vulnerability is typically chained with a companion flaw, CVE-2026-72529, which lets an attacker first execute an arbitrary script inside the isolated environment by calling an undocumented function. The combination gives an attacker full, unauthenticated, highest-privilege control of the server with no user interaction required.
TrueConf fixed both flaws in versions 5.3.9, 5.4.9, and 5.5.5, released 18 June 2026 after private notification from Kaspersky.

What are the systems affected?

Affected systems are on-premise TrueConf Server deployments on Windows or Linux. Organisations that do not run TrueConf themselves should still note the indirect exposure path described below.

TrueConf Server, all versions prior to 5.3 - (Affected)
TrueConf Server 5.3.x, prior to 5.3.9 - (Affected)
TrueConf Server 5.4.x, prior to 5.4.9 - (Affected)
TrueConf Server 5.5.x, prior to 5.5.5 - (Affected)
TrueConf Server 5.3.9, 5.4.9, 5.5.5 and later - (Not affected, patched)

Even organisations that do not run TrueConf Server themselves should be aware that any staff member who joins a video conference hosted on a third party's compromised TrueConf server may be served a trojanised client installer.

What does this mean?

This flaw requires no initial access step: the only prerequisite is unauthenticated network reachability to TCP port 4307, which is open by default.

Step 1 - Unauthenticated Network Access
The attacker connects to TCP port 4307 on the target TrueConf server, which requires no authentication and is exposed by default.

Step 2 - Script Execution Inside the Sandbox (CVE-2026-72529)
The attacker calls an undocumented function to execute an arbitrary script within TrueConf's isolated execution environment.

Step 3 - Sandbox Escape (CVE-2026-72530)
A second, specially crafted script exploits this vulnerability to break out of the isolated environment entirely, achieving code execution on the underlying host operating system with the highest available privileges.

Step 4 - Supply-Chain Poisoning and Backdoor Delivery
Observed intrusions deploy a PHP web shell to maintain access and gain privileged access to the TrueConf database, then replace the server's legitimate client installer with a **trojanised, non-digitally signed version**. Any user connecting to the server for an update unknowingly installs the PhantomCore and PhantomGraph backdoors, which have been used for LSASS credential dumping, reconnaissance, and reverse SSH tunnelling.

Mitigation process

CERTVU recommends the following:

1. **Update TrueConf Server Immediately**

Update TrueConf Server to version 5.3.9, 5.4.9, or 5.5.5, whichever corresponds to the deployed branch. Given confirmed active exploitation by an advanced persistent threat actor and the potential for full, highest-privilege compromise of the server, treat any unpatched, network-reachable TrueConf Server as an emergency rather than a scheduled update.

Kaspersky ICS CERT Advisory KLCERT-26-058

2. **Assume Compromise and Check Client Installers**

Any TrueConf server that was unpatched and reachable on TCP port 4307 should be treated as potentially compromised. Perform a full scan with up-to-date antivirus software, and check for indicators of compromise associated with the Head Mare/PhantomCore campaign, including an unauthorised PHP web shell, a rogue administrative account, and a non-digitally signed TrueConf Client installer replacing the legitimate one.

Reference

1. https://ics-cert.kaspersky.com/advisories/2026/08/11/trueconf-server-breakout-from-isolated-environment/
2. https://www.cve.org/CVERecord?id=CVE-2026-72530
3. https://ics-cert.kaspersky.com/publications/reports/2026/08/12/head-mare-exploits-vulnerabilities-in-trueconf-server-to-deliver-phantomcore-malware/
4. https://thehackernews.com/2026/08/head-mare-exploits-trueconf-flaws-to.html

.