

CVE-2026-72529

TrueConf Server Missing Authentication for Critical Function Vulnerability

CISA KEV since Aug 20, 2026

Actively exploited

A remote unauthorized attacker with network access via port 4307/TCP to the TrueConf server versions 5.3.X to 5.3.9, 5.4.X to 5.4.9, 5.5.X to 5.5.5, and earlier could execute an arbitrary script by calling an undocumented function.

EVRS 75 _{/100} Urgent priority	CVSS V4.0 9.3 Critical · NVD	EPSS 0.015 73.4th percentile · FIRST	CISA DEADLINE Aug 23, 2026 CISA federal deadline · Overdue by 2 months
--	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☒ KEV recency	Added to CISA KEV within the last 90 days
☒ EPSS	0.015 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
trueconf server	< 5.3.9.10013 < 5.3.9.10015 ≥ 5.4.0.12689 < 5.4.9.10072 ≥ 5.4.0.12700 < 5.4.9.10019 ≥ 5.5.0.13826 < 5.5.5.10010 ≥ 5.5.0.13828 < 5.5.5.10009	5.3.9.10013 · 5.3.9.10015 · 5.4.9.10072 · 5.4.9.10019 · 5.5.5.10010 · 5.5.5.10009	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-xc2x-q39j-746f	trueconf.com	trueconf.com/blog/news/security-fixes-updates-and-advisories
ics-cert.kaspersky.com	ics-cert.kaspersky.com/advisories/2026/08/11/trueconf-server-missing-authentication-for-critical-function/	BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk
Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk	NVD	nvd.nist.gov/vuln/detail/CVE-2026-72529
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-62587
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-72529		



Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.