

CVE-2025-54948

Trend Micro Apex One OS Command Injection Vulnerability

CISA KEV since Aug 18, 2025

Actively exploited

A vulnerability in Trend Micro Apex One (on-premise) management console could allow a pre-authenticated remote attacker to upload malicious code and execute commands on affected installations.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.239 97.8th percentile · FIRST	CISA DEADLINE Sep 8, 2025 KEV since 2025 · listed over a year
---	--	--	---

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 two years
☒ EPSS	0.239 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** N/A

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
apex one	2019	no fixed version listed	NVD

Sources

Vendor guidance	success.trendmicro.com/en-US/solution/KA-0020652	NVD	nvd.nist.gov/vuln/detail/CVE-2025-54948
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-23621
Current data	evulnable.com/vulnerability-management/cve/CVE-2025-54948		

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