Computer Emergency Response Team of Mauritius
A department under the Ministry of Information Technology, Communication and Innovation

CERT-MU Security Advisory

CERT-MU Advisories AD-2025-05

Trend Micro Apex One Vulnerability

Date of Issue: 19 August 2025

Severity Rating: High

Systems Affected:

- Trend Micro Apex One Management Console (on-premise)

CVE Information:

- CVE-2025-54948

Description

A vulnerability was identified in Trend Micro Apex One Management Console's on-premise deployments and poses significant risks to organizations worldwide. The vulnerability consists of a severe OS command injection flaw within Trend Micro's Apex One Management Console, and this could allow pre-authenticated remote attackers to upload malicious code and execute arbitrary commands on affected installations.

Technical details

This type of vulnerability, categorized under CWE-78 (OS Command Injection), enables attackers who have already gained initial access to escalate their privileges and potentially compromise entire network infrastructures. The flaw requires pre-authentication, meaning attackers must first obtain valid credentials or exploit another vulnerability to gain initial access before leveraging CVE-2025-54948.

However, once exploited, the vulnerability provides attackers with powerful capabilities to execute system-level commands, potentially leading to complete system compromise.

Impact

Although it has not been confirmed yet, the vulnerability can be used in ransomware campaigns. The combination of command injection capabilities and enterprise security platform access makes CVE-2025-54948 particularly attractive to ransomware operators seeking to disable security controls and establish persistence within targeted networks.

Mitigation

Organisations should monitor threat intelligence feeds for updates regarding potential ransomware exploitation and implement additional security measures around their Apex One deployments while awaiting vendor patches.

Organisations using Trend Micro Apex One should immediately consult vendor security advisories, implement recommended mitigations, and consider additional monitoring around affected systems until comprehensive patches become available**.**

References

https://www.helpnetsecurity.com/2025/08/06/trend-micro-apex-one-flaws-exploted-in-the-wild-cve-2025-54948-cve-2025-54987/

Postal address

Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,
Cybercity Ebene,