THREAT BULLETINS

Trend Micro Discloses Two Exploited Critical Flaws (CVE-2025-54948 and CVE-2025-54987)

TLP:WHITE

Aug 06, 2025

On August 5, Trend Micro issued an urgent security advisory for two critical vulnerabilities, CVE-2025-54948 and CVE-2025-54987, affecting on-premise versions of its Apex One Management Console. TrendMicro has observed at least one attempt to exploit these vulnerabilities in the wild.

Both flaws are pre-authenticated remote code execution and command injection vulnerabilities. Threat actors could use these flaws to upload malicious code and execute commands on the affected server. The flaws are essentially the same, with the only difference being that they target different CPU architectures. The assigned CVSS score is 9.4 for both flaws, highlighting their criticality.

To exploit these flaws, threat actors would need access to the Trend Micro Apex One Management Console. This puts customers whose IP addresses are exposed externally at a higher risk. As a mitigation, these customers are advised to implement source restrictions. TrendMicro has released temporary fixes; a more formal patch is expected for mid-August.

Reference(s)	thehackernews, trendmicro, cybersecuritynews, securityonline

Sources
https://success.trendmicro.com/en-US/solution/KA-0020652

https://thehackernews.com/2025/08/trend-micro-confirms-active.html

https://securityonline.info/critical-command-injection-flaws-in-trend-micro-apex-one-actively-exploited/

https://cybersecuritynews.com/trend-micro-apex-one-rce-vulnerability/

Recommendations

- Apply short-term patches and follow Trend Micro's advisory for updates.
- Implement source restrictions to protect externally exposed IP addresses.
- Enforce network segmentation and strict network access control policies.
- Implement multi-factor authentication for accounts across the organization.
- Continuously monitor for suspicious activities, including unauthorized access and unusual appliance logs or connections.
- Have an incident response plan ready to limit operational disruptions in the event of a successful attack.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients resources.

Incident Date
Aug 05, 2025 (UTC)

Alert ID 945ca9ff

View Alert

Share Feedback

was this helpful? |

Tags Apex One Management Console, CVE-2025-54987, CVE-2025-54948, Trend Micro

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**