Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Trend Micro Warns of Active Exploits in Apex One Console

Date of Publication	Admiralty Code	TA Number
August 7, 2025	A1	TA2025242

Summary

First Seen: August 2025
Affected Product: Trend Micro Apex One
Impact: Trend Micro has identified two serious zero-day vulnerabilities in its Apex One On-Premise Management Console one of which is currently being exploited in the wild. These flaws could allow attackers to remotely run malicious code on affected systems without needing to log in. To protect users, Trend Micro has released a temporary fixtool that blocks the attack, though it disables some remote features. A permanent fix is expected to arrive by mid-August 2025. In the meantime, users are strongly urged to apply the fixtool.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-54948	Trend Micro Apex One Management Console Command Injection RCE Vulnerability	Trend Micro Apex One Management Server Version 14039 and below	✓	✗	✗
CVE-2025-54987	Trend Micro Apex One Management Console Command Injection RCE Vulnerability	Trend Micro Apex One Management Server Version 14039 and below	✓	✗	✗

Vulnerability Details

#1

Trend Micro has disclosed two critical zero-day vulnerabilities affecting the on-premise version of its Apex One Management Console. These flaws tracked as CVE-2025-54948 and CVE-2025-54987, and one of which have reportedly been exploited in the wild, putting enterprise systems at immediate risk. Apex One is widely used for endpoint protection across desktops, laptops, and servers, and these vulnerabilities expose its management interface to remote code execution attacks without requiring prior authentication.

#2

Both vulnerabilities stem from improper validation of user-supplied input within the Apex One console, which listens on TCP ports 8080 and 4343 by default. An attacker could exploit these flaws by uploading malicious code and triggering a system call, resulting in arbitrary command execution under the IUSR user context. While the two CVEs are technically similar, CVE-2025-54987 targets a different CPU architecture, expanding the attack surface and potentially affecting a broader range of deployments.

#3

In response, Trend Micro has released a mitigation tool designed to block these command injection vulnerabilities. However, applying this temporary fix disables the Remote Install Agent feature, which may impact remote management operations. A Critical Patch is scheduled for release by mid-August 2025, which will not only fully address the vulnerabilities but also restore any functionality disabled by the mitigation tool. This patch is expected to serve as the permanent solution for affected systems.

#4

Until the patch becomes available, all users using Apex One On-Premise are urged to immediately deploy the provided fixtool. Despite the inconvenience of losing some remote capabilities, the company emphasizes that securing vulnerable endpoints should take precedence given the confirmed exploitation in the wild. Administrators are advised to remain vigilant and prioritize endpoint protection while waiting for the official security update.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-54948	Trend Micro Apex One Management Server Version 14039 and below	cpe:2.3:a:trendmicro:apexone:*:*:*:*:*:*:*:*	CWE-78
CVE-2025-54987	Trend Micro Apex One Management Server Version 14039 and below	cpe:2.3:a:trendmicro:apexone:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Apply the Mitigation Tool Immediately: Apply to the temporary fix (fixtool) released by Trend Micro to block these actively exploited vulnerabilities. Even though it disables some remote features, it's crucial to apply it right away to protect your systems from potential attacks.

Limit Remote Access to the Console: Until the official patch arrives, consider restricting access to the Apex One Management Console, especially from untrusted networks. This reduces the chances of an attacker reaching the vulnerable interface.

Monitor Systems for Suspicious Activity: Keep an eye on your systems for any unusual behavior or unauthorized access attempts. Since these vulnerabilities are already being exploited, it's wise to increase monitoring until the issue is fully resolved.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	T1588 Obtain Capabilities	T1588.006 Vulnerabilities
T1059 Command and Scripting Interpreter	T1203 Exploitation for Client Execution		

Patch Details

If you're using Trend Micro Apex One On-Premise, it's strongly recommended to apply the fixtool right away. A permanent patch is expected by mid-August 2025.

References

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

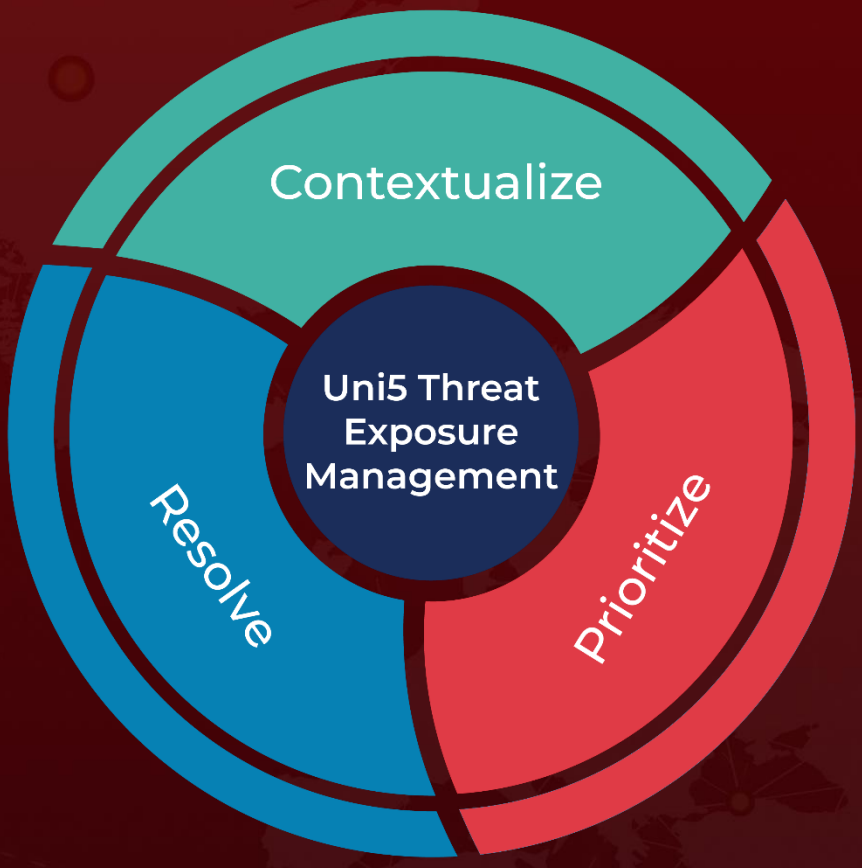
https://www.zerodayinitiative.com/advisories/ZDI-25-771/

https://www.zerodayinitiative.com/advisories/ZDI-25-772/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 7, 2025 . 5:50 AM

More at www.hivepro.com