مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in Trend Micro Apex One On-Premise

Tracking #:432319014

Date:22-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Trend Micro have disclosed multiple security vulnerabilities including an actively exploited vulnerability.

TECHNICAL DETAILS:

Trend Micro have disclosed multiple security vulnerabilities affecting:

- TrendAI Apex One
- Trend Micro Apex One as a Service
- TrendAI Vision One Endpoint Security - Standard Endpoint Protection

One of the vulnerabilities, tracked as CVE-2026-34926, is reportedly being actively exploited in the wild. Successful exploitation could allow authenticated attackers to tamper with arbitrary files, distribute malicious code to security agents, or escalate privileges within affected environments.

Exploited Vulnerability

- CVE ID: CVE-2026-34926
- Vulnerability Type: Relative Path Traversal
- Affected Product: TrendAI Apex One (On Premise)

Other Vulnerabilities:

1. CVE ID: CVE-2026-34927
   - Vulnerability Type: Origin Validation Error Local Privilege Escalation
   - Affected Product: TrendAI Apex One / TrendAI Vision One Endpoint Security - Standard Endpoint Protection
   - CVSS v3.1: 7.8 High
2. CVE ID: CVE-2026-34928
   - Vulnerability Type: Origin Validation Error Local Privilege Escalation
   - Affected Product: TrendAI Apex One / TrendAI Vision One Endpoint Security - Standard Endpoint Protection
   - CVSS v3.1: 7.8 High
3. CVE ID: CVE-2026-34929
   - Vulnerability Type: Origin Validation Error Local Privilege Escalation
   - Affected Product: TrendAI Apex One / TrendAI Vision One Endpoint Security - Standard Endpoint Protection
   - CVSS v3.1: 7.8 High
4. CVE ID: CVE-2026-34930
   - Vulnerability Type: Origin Validation Error Local Privilege Escalation
   - Affected Product: TrendAI Apex One / TrendAI Vision One Endpoint Security - Standard Endpoint Protection
   - CVSS v3.1: 7.8 High
5. CVE ID: CVE-2026-45206
   - Vulnerability Type: Origin Validation Error Local Privilege Escalation
   - Affected Product: TrendAI Apex One / TrendAI Vision One Endpoint Security - Standard Endpoint Protection
   - CVSS v3.1: 7.8 High
6. CVE ID: CVE-2026-45207
   - Vulnerability Type: Origin Validation Error Local Privilege Escalation

- Affected Product: TrendAI Apex One / TrendAI Vision One Endpoint Security - Standard Endpoint Protection
- CVSS v3.1: 7.8 High

7. CVE ID: CVE-2026-45208
   - Vulnerability Type: Time-of-Check Time-of-Use (TOCTOU) Local Privilege Escalation
   - Affected Product: TrendAI Apex One / TrendAI Vision One Endpoint Security - Standard Endpoint Protection
   - CVSS v3.1: 7.8 High

RECOMMENDATIONS:

- Patch affected Trend Micro products without delay
- Upgrade all endpoint security agents to the latest available version
- Identify systems running vulnerable Apex One On Premise deployments
- Validate integrity of management servers and deployed agents

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://success.trendmicro.com/en-US/solution/KA-0023430