

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Multiple Vulnerabilities in Trend Micro Apex Central
Tracking #:432318232
Date:12-01-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Trend Micro has released a critical security update for Trend Micro Apex Central (on-premise) to address multiple high and critical-severity vulnerabilities. These issues could allow unauthenticated remote attackers to execute arbitrary code with SYSTEM-level privileges or cause denial-of-service (DoS) conditions.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2025-69258 – Remote Code Execution**
 - **CVSS v3.1:** 9.8 **Critical**
 - A LoadLibraryEX flaw could allow an unauthenticated remote attacker to load a malicious DLL, resulting in arbitrary code execution with SYSTEM-level privileges.
- **CVE-2025-69259 – Denial of Service**
 - **CVSS v3.1:** 7.5 High
 - An unchecked NULL return value vulnerability could allow a remote attacker to trigger a denial-of-service condition.
- **CVE-2025-69260 – Denial of Service**
 - **CVSS v3.1:** 7.5 High
 - An out-of-bounds read vulnerability could allow a remote attacker to cause a denial-of-service condition.

Affected Versions

- **Product:** Trend Micro Apex Central (on-premise)
- **Affected Versions:** All versions **below Build 7190**
- **Platform:** Windows

Fixed Versions

- Trend Micro Apex Central (on-premise): Critical Patch Build 7190 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Trend Micro.

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-0022071>