مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Trend Micro Cloud Edge

Tracking #:432316401

Date:16-10-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Trend Micro Cloud Edge that could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-48904**
- CVSSv3 score 9.8 Critical
- A critical command injection flaw in **Trend Micro Cloud Edge**, which allows remote attackers to execute arbitrary code on affected appliances without requiring authentication.
- Exploiting this command injection vulnerability typically requires that an attacker has either physical or remote access to the vulnerable machine. The nature of command injection vulnerabilities allows attackers to manipulate system commands, potentially leading to full remote code execution (RCE) on the affected systems.

Affected Versions:

- Cloud Edge 5.6 SP2
- Cloud Edge 7.0

Fixed Versions:

- Cloud Edge 5.6 SP2 build 3228
- Cloud Edge 7.0 build 1081

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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-0017998