مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# High-Severity Vulnerability in ManageEngine Log360

Tracking #:432318805

Date:17-04-2026

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity authentication bypass vulnerability in ManageEngine Log360. This flaw may allow unauthorized users to access sensitive data and perform restricted operations through exposed APIs.

## TECHNICAL DETAILS:

**Vulnerability Details**

- **CVE ID:** CVE-2026-3324
- **Severity:** High
- The vulnerability exists due to improper authorization checks in exposed V1 APIs. An attacker can exploit this flaw to bypass authentication mechanisms, potentially gaining unauthorized access to system data and functionality.

**Affected Products**

- **ManageEngine Log360**
- Builds **13000 to 13013**

**Fixed Version**

- upgrade to build 13017 or later

## RECOMMENDATIONS:

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

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://www.manageengine.com/log-management/advisory/CVE-2026-3324.html