مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in IBM Tivoli Monitoring

Tracking #:432317328

Date:30-05-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability in IBM Tivoli Monitoring that could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

IBM Tivoli Monitoring has identified and remediated a critical vulnerability related to improper validation of input data. This security flaw, tracked as **CVE-2025-3357**, could potentially allow a remote attacker to execute arbitrary code under certain conditions.

Vulnerability Details:

- CVE-2025-3357
- CVSS Base Score: 9.8 (Critical)
- IBM Tivoli Monitoring is vulnerable to improper validation of an index value in a dynamically allocated array, which may allow an attacker to execute arbitrary code remotely.
- Exploitation of this vulnerability can lead to:
  - Full system compromise
  - Data theft or loss
  - Service disruption
  - Lateral movement within the network

Affected Products and Versions:

- IBM Tivoli Monitoring versions **6.3.0.7 through 6.3.0.7 Service Pack 19**

Remediation and Fixes:

- Upgrade to latest available service pack: **IBM Tivoli Monitoring Service Pack 6.3.0.7-TIV-ITM-SP0020** (VRMF: 6.3.0.7).

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by IBM.

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.ibm.com/support/pages/node/7234923