مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Ivanti Endpoint Manager 2024

Tracking #:432318387

Date:11-02-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Ivanti has released a security update addressing multiple vulnerabilities in Ivanti Endpoint Manager that could allow remote attackers to compromise systems and exfiltrate sensitive data.

TECHNICAL DETAILS:

Ivanti has released a security update (version 2024 SU5) addressing multiple vulnerabilities in Ivanti Endpoint Manager that could allow remote attackers to compromise systems and exfiltrate sensitive data. The most severe vulnerability (CVE-2026-1603) is rated 8.6 HIGH and permits unauthenticated attackers to bypass authentication and leak stored credential data. A second vulnerability (CVE-2026-1602) enables authenticated attackers to execute SQL injection attacks to read arbitrary database information.

Key Points:

- Two newly disclosed vulnerabilities (1 High, 1 Medium severity)
- Additional 11 medium severity vulnerabilities from October 2025 resolved

VULNERABILITY DETAILS

1. CVE-2026-1603: Authentication Bypass Leading to Credential Exposure

- **Severity:** HIGH (CVSS 8.6)

2. CVE-2026-1602: SQL Injection Vulnerability

- **Severity:** MEDIUM (CVSS 6.5)

AFFECTED SYSTEMS

- Affected Product: Ivanti Endpoint Manager (EPM)
- Affected Versions: 2024 SU4 SR1 and all prior versions
- Fixed Version: 2024 SU5

RECOMMENDATIONS:

- Apply Security Updates and Prioritize internet-facing or publicly accessible EPM installations.

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://hub.ivanti.com/s/article/Security-Advisory-EPM-February-2026-for-EPM-2024?language=en_US