

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Multiple Vulnerabilities in Ivanti Endpoint Manager (EPM)

Tracking #:432317057

Date:10-04-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Ivanti has disclosed multiple vulnerabilities affecting its Endpoint Manager (EPM) products.

TECHNICAL DETAILS:

Ivanti has released a security advisory addressing six vulnerabilities affecting Ivanti Endpoint Manager (EPM) versions 2022 SU6 and earlier, and 2024 prior to SU1. These vulnerabilities include high-severity issues such as privilege escalation via DLL hijacking, SQL injection allowing code execution, and reflected cross-site scripting (XSS) enabling administrative takeover through user interaction. Medium-severity issues include local denial-of-service and improper certificate validation.

Vulnerability Details:

CVE ID	Description	Severity	CVSS v3.0 Score
CVE-2025-22464	Local untrusted pointer dereference could allow DoS via memory manipulation.	Medium	6.1
CVE-2025-22465	Reflected XSS allows remote attacker to execute arbitrary JavaScript in the victim's browser.	Medium	6.1
CVE-2025-22466	Reflected XSS enables remote privilege escalation to admin. User interaction required.	High	8.2
CVE-2025-22458	DLL hijacking vulnerability may lead to SYSTEM-level privilege escalation.	High	7.8
CVE-2025-22459	Improper certificate validation allows MITM interception of limited traffic.	Medium	4.8
CVE-2025-22461	SQL injection allows remote code execution for authenticated admin users.	High	7.2

Affected Versions:

Product Name	Affected Version(s)	Resolved Version(s)
Ivanti Endpoint Manager	2022 SU6 and earlier	2022 SU7
Ivanti Endpoint Manager	2024	2024 SU1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade Ivanti Endpoint Manager to fixed version 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://forums.ivanti.com/s/article/Security-Advisory-EPM-April-2025-for-EPM-2024-and-EPM-2022-SU6?language=en_US&gl=1*10zbgk3*_gcl_au*NDM4ODA2NzI5LjE3NDE3MDI4ODA.