مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Ivanti Endpoint Manager
Tracking #:432317811
Date:14-10-2025

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Ivanti has disclosed multiple security vulnerabilities affecting Ivanti Endpoint Manager (EPM), including two high-severity and eleven medium-severity flaws.

TECHNICAL DETAILS:

Ivanti has disclosed multiple security vulnerabilities affecting Ivanti Endpoint Manager (EPM), including two high-severity and eleven medium-severity flaws. Successful exploitation could enable privilege escalation or remote code execution (RCE) on affected systems. While no active exploitation has been observed at the time of publication, these vulnerabilities pose a significant risk to enterprise environments leveraging Ivanti EPM for endpoint management.

High Severity Vulnerability Details:
1. CVE-2025-11622- 7.8 (High)-Insecure deserialization in Ivanti Endpoint Manager allows a local authenticated attacker to escalate their privileges.
2. CVE-2025-9713 8.8 (High) -Path traversal in Ivanti Endpoint Manager allows a remote unauthenticated attacker to achieve remote code execution. User interaction is required.

Affected Versions:

Product Name	Affected Version(s)	Resolved Version(s)	Patch Availability
Ivanti Endpoint Manager	2024 SU3 SR1 and prior	CVE-2025-11622 & CVE-2025-9713: will be resolved in 2024 SU4 version targeted for November 12, 2025. CVE-2025-11623, CVE-2025-62392, CVE-2025-62390, CVE-2025-62389, CVE-2025-62388, CVE-2025-62387, CVE-2025-62385, CVE-2025-62391, CVE-2025-62383, CVE-2025-62386, CVE-2025-62384: will be resolved in 2024 SU5 version targeted for Q1 2026	Patches are currently in development. Customers should refer to the mitigations to protect their environment.
Ivanti Endpoint Manager	2022 SU8 SR2 and prior	N/A	This version is End of Life. Customers should move to the latest version of Ivanti EPM 2024 to significantly reduce their risk.

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

RECOMMENDATIONS:

TLP: WHITE

- Monitor Vendor Updates: Follow Ivanti's official advisories for patch release notifications.
- Organizations should prioritize upgrading to supported versions and implement the recommended mitigations immediately.

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-Ivanti-Endpoint-Manager-EPM-October-2025?language=en_US