مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Privilege Escalation Vulnerability in Ivanti Neurons for ITSM

Tracking #:432319049

Date:02-06-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Ivanti Neurons for ITSM. This vulnerability could allow authenticated attackers to escalate privileges and obtain administrative access in affected environments.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-9614**
- **Severity / CVSS:** High — CVSS 8.8
- An improper access control vulnerability exists in Ivanti Neurons for ITSM that could allow a remote authenticated attacker with low privileges to gain administrative access within affected environments.
- Successful exploitation could enable attackers to obtain administrative privileges, potentially resulting in unauthorized access to sensitive information, modification of system configurations, disruption of services, and further compromise of the affected environment.

Affected Products and Versions

- **Ivanti Neurons for ITSM (On-Premises)**: Affected Versions: 2025.4 and earlier
- **Ivanti Neurons for ITSM (Cloud)**: Affected Versions: 2026.1 and earlier

Fixed Versions

On-Premises Deployments:

- 2025.4 Patch 1
- 2025.3 Patch 1
- 2025.2 Patch 1

Cloud Deployments:

- Fixed in 2026.1 Patch 9
- Fixed in 2026.2 Patch 1

Note: Ivanti stated that security updates were automatically applied to cloud environments and no action is required.

RECOMMENDATIONS:

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

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-Ivanti-Neurons-for-ITSM-CVE-2026-9614?language=en_US