مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Juniper JSI vLWC

Tracking #:432318762

Date:10-04-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Juniper Networks Support Insights Virtual Lightweight Collector (vLWC). This flaw could allow unauthenticated attackers to gain full control of affected systems over the network.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE ID:** CVE-2026-33784
- **Severity:** Critical **CVSS:** 9.8
- The vulnerability is caused by the presence of a default password assigned to a high-privileged account in vLWC deployments. Since the system does not enforce a password change during provisioning, attackers can exploit this weakness to authenticate remotely without credentials and obtain full administrative access. Successful exploitation could result in complete compromise of the affected device, including unauthorized configuration changes, data access, and service disruption.

Affected Versions

- All versions of Juniper Networks Support Insights (JSI) vLWC prior to version 3.0.94

Fixed Versions

- Juniper Networks Support Insights (JSI) vLWC version 3.0.94 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Juniper Networks.

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://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-vLWC-Default-password-is-not-required-to-be-changed-which-allows-unauthorized-high-privileged-access-CVE-2026-33784