



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerability in Versa Director

Tracking #:432316541

Date:21-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Versa Networks has issued a critical security advisory concerning a vulnerability in the Versa Director software.

TECHNICAL DETAILS:

Versa Networks has issued a critical security advisory concerning a vulnerability (CVE-2024-42450) in the Versa Director software.

Vulnerability Details:

- **Vulnerability Identifier:** CVE-2024-42450
- **Severity:** **Critical** (CVSS 10)
- **Vulnerable Product:** **Versa Director**
- The vulnerability arises from the default configuration of PostgreSQL (Postgres), which is used by Versa Director for storing operational and configuration data. Specifically, Postgres is configured to listen on all network interfaces by default, and the use of a common default password exposes the database to potential attackers. This configuration allows an unauthenticated attacker to connect to the database, escalate privileges, and access or modify sensitive data, leading to potential remote code execution.

Affected Versions:

- 22.1.4-images released before November 11, 2024
- 22.1.3
- 22.1.2
- 22.1.1
- 21.2.3
- 21.2.2

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to immediately update to Versa Director the latest release.

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://security-portal.versa-networks.com/emailbulletins/6735a300415abb89e9a8a9d3>