مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Vulnerability in Versa Director

Tracking #:432316325

Date:25-09-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Versa Networks has released an advisory for a vulnerability affecting Versa Director.

TECHNICAL DETAILS:

Versa Networks has released an advisory for a vulnerability (CVE-2024-45229) affecting Versa Director. The Versa Director offers REST APIs for orchestration and management. By design, certain APIs, such as the login screen, banner display, and device registration, do not require authentication. However, it was discovered that for Directors directly connected to the Internet, one of these APIs can be exploited by injecting invalid arguments into a GET request, potentially exposing the authentication tokens of other currently logged-in users. These tokens can then be used to invoke additional APIs on port 9183. This exploit does not disclose any username or password information.

Versions	Affected	Unaffected
22.1.4	22.1.4 images released before September 9, 2024	22.1.4 September 12, 2024 Hot Fix and later.
22.1.3	22.1.3 images released before September 9, 2024	22.1.3 September 12, 2024 Hot Fix and later.
22.1.2	22.1.2 images released before September 9, 2024	22.1.2 September 12, 2024 Hot Fix and later.
22.1.1	All	Please upgrade to 22.1.3 latest version.
21.2.3	21.2.3 images released before September 9, 2024	21.2.3 September 12, 2024 Hot Fix and later.
21.2.2	All	Please upgrade to 21.2.3 latest version.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update the affected versions to latest 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://security-portal.versa-networks.com/emailbulletins/66e4a8ebda545d61ec2b1ab9