مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Nginx UI

Tracking #:432318553

Date:10-03-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been identified in Nginx UI that allows unauthenticated attackers to download and decrypt full system backups from affected servers.

TECHNICAL DETAILS:

A critical vulnerability has been identified in Nginx UI that allows unauthenticated attackers to download and decrypt full system backups from affected servers. The vulnerability, tracked as CVE-2026-27944, has been assigned a CVSS score of 9.8 (Critical).
The flaw enables attackers to retrieve sensitive data including user credentials, system configuration files, session tokens, and SSL/TLS private keys, potentially allowing full compromise of the affected server environment.

Vulnerability Details
Vulnerability Identifier

- CVE-2026-27944

Severity

- Critical (CVSS Score: 9.8)

Affected Product

- Nginx UI

Affected Versions

- Versions prior to 2.3.2

Patched Version

- Version 2.3.3

RECOMMENDATIONS:

Immediate Mitigation

- Upgrade Nginx UI version to fixed version or later.

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://github.com/0xJacky/nginx-ui/security/advisories/GHSA-g9w5-qffc-6762