مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in SolarWinds Observability Self-Hosted

Tracking #:432317550
Date:30-07-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in SolarWinds Observability Self-Hosted (SWOSH) that could allow an attacker to gain elevated privileges, potentially compromising system confidentiality, integrity, and availability.

TECHNICAL DETAILS:

Vulnerability Details:

- **Vulnerability ID:** CVE-2025-26397
- **CVSS Score:** 7.8 (High)
- A security vulnerability exists in SolarWinds Observability Self-Hosted (SWOSH), which may allow local attackers with low-level credentials to escalate privileges on the host system. The issue stems from a Deserialization of Untrusted Data flaw, enabling execution of malicious files within permission-protected folders.
- Exploitation requires authenticated access and local presence on the target system.
- Successful exploitation could allow an attacker to gain elevated privileges, potentially compromising system confidentiality, integrity, and availability.

Affected Versions:

- SWOSH 2025.2 and prior versions

Fixed Version:

- SWOSH 2025.2.1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the latest updates released by SolarWinds 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://www.solarwinds.com/trust-center/security-advisories/cve-2025-26397