مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in SolarWinds Platform

Tracking #:432316865

Date:13-02-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the SolarWinds Platform that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-52612**
- CVSS Score 6.8 High
- SolarWinds Platform is vulnerable to a reflected cross-site scripting (XSS) vulnerability. The vulnerability stems from insufficient sanitation of input parameters and requires authentication by a high-privileged account to be exploitable.
- The reflected XSS vulnerability in SolarWinds Platform allows an authenticated attacker with high privileges to potentially execute arbitrary scripts. This flaw affects the search and node information sections of the user interface.
- Successful exploitation of this vulnerability could lead to:
    - Unauthorized execution of scripts
    - Session hijacking
    - Potential access to sensitive information

Affected Versions:

- SolarWinds Platform 2024.2.1 and older versions

Fixed Versions:

- SolarWinds Platform 2025.1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by SolarWinds.

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-2024-52612