مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in SolarWinds DameWare Mini Remote Control

Tracking #:432317347

Date:04-06-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity Vulnerability in SolarWinds DameWare Mini Remote Control that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- CVE-2025-26396
- Severity: High (CVSS v3.1: 7.8)
- A local privilege escalation vulnerability exists in SolarWinds DameWare Mini Remote Control. This vulnerability is caused by incorrect file or folder permissions, allowing a local attacker with a valid low-privilege account to escalate privileges and execute code as SYSTEM.
- Successful exploitation could grant attackers SYSTEM-level privileges, enabling full control over the affected system.

Affected Products:

- SolarWinds DameWare Mini Remote Control 12.3.1.20 and earlier

Fixed Version:

- Dameware Mini Remote Control 12.3.2

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-2025-26396