**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

**GOUVERNEMENT DE LA
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

16 March 2026

Advisory 122: SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability

Release Date: 09th March 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

Communication and Digital Transformation (DCDT through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2025-26399 is a critical remote code execution (RCE) vulnerability affecting the SolarWinds Web Help Desk platform. The vulnerability arises from deserialization of untrusted data (CWE-502) in the AjaxProxy component**,** which fails to properly validate user-supplied input before processing it.

What are the systems affected?

The vulnerability affects installations of:

- **SolarWinds Web Help Desk**
- **Version 12.8.7 and earlier releases** of the software.

Web Help Desk is widely used by organizations for:

- IT service management (ITSM)
- Help desk ticketing systems
- Asset and incident management

Because the platform is typically deployed on internal enterprise servers, exploitation can compromise critical internal infrastructure

What does this mean?

Attackers exploit the vulnerability through malicious serialized data sent to the AjaxProxy endpoint of the application.

Mitigation process

CERTVU recommends the following:

1. Apply Vendor Security Updates:

- SolarWinds Web Help Desk 12.8.7 Hotfix 1 (HF1**)** or later.

2. Restrict External Access (If immediate patching is not possible):

- Limit Web Help Desk access to internal networks or VPN only
- Block public access via firewall rules.

Reference

.

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2025-26399