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

23 April 2026

Advisory 137: Microsoft SharePoint Server Improper Input Validation Vulnerability (CVE-2026-32201).

Release Date: 14th April 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communications 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?

Microsoft SharePoint Server contains an improper input validation vulnerability that allows an unauthorized attacker to perform spoofing over a network.

What are the systems affected?

The vulnerability affects older Microsoft Products including:

- Microsoft SharePoint Enterprise Server 2016 (x64-based System)
  - Version affected from 16.0.0 before 16.0.5548.1003
- Microsoft SharePoint Server 2019 (x64-based System)
  - Version affected from 16.0.0 before 16.0.10417.20114
- Microsoft SharePoint Server Subscription Edition (x64-based System)
  - Version affected from 16.0.0 before 16.0.19725.20210

What does this mean?

Exploitation is network-based and does not require prior authentication**.**

Typical attack flow:

1. **Target identification**
    - Attacker locates exposed SharePoint servers on internal or external networks.
2. **Crafted request submission**
    - Malicious HTTP requests are sent with manipulated or malformed input fields**.**
3. **Bypassing input validation**
    - The server fails to properly validate or sanitize the input.
4. **Request or identity spoofing**
    - The system incorrectly interprets the attacker's input as trusted data, allowing:
        - Forged user identities
        - Manipulated session or request context
        - Unauthorized actions performed as another user or system component

Mitigation process

CERTVU recommends the following:

Apply Microsoft Security Updates (Critical)

- Install the latest SharePoint Server security patches provided by Microsoft
- Ensure all farm servers are updated consistently

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-32201
3. https://cwe.mitre.org/data/definitions/20.html
4. https://learn.microsoft.com/en-us/officeupdates/sharepoint-updates

.