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

25 March 2026

Advisory 124: Microsoft SharePoint Deserialization of Untrusted Data Vulnerability

Release Date: 18th 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-2026-20963 is a high-severity remote code execution (RCE) vulnerability (CVSS 8.8) affecting Microsoft SharePoint Server. The flaw is caused by deserialization of untrusted data (CWE-502) within SharePoint's handling of serialized objects.

What are the systems affected?

The Vulnerability impacts on premises SharePoint deployments, including:

- Microsoft SharePoint Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Subscription Edition (prior to patched builds)

These systems are commonly used in enterprise environments for:

- Document Management
- Collaboration platforms
- Internal portals and knowledge repositories

What does this mean?

Exploitation requires low-privileged authenticated access, meaning even a normal user account can be leveraged.

The attack is network-based, low complexity, and requires no user interaction, making it highly exploitable.

Typical attack flow:

1. Initial access (low privilege)
    - The attacker gains valid SharePoint credentials (e.g., phishing or insider access).
2. Crafting malicious payload
    - The attacker creates a specially crafted serialized object payload designed to exploit deserialization logic.
3. Sending the request
    - The payload is sent to a vulnerable SharePoint endpoint that processes serialized data.
4. Unsafe deserialization
    - SharePoint deserializes the malicious object without validation.
5. Code execution
    - The payload triggers execution of attacker-controlled code on the server.
6. Post-exploitation
    - Attackers may:
        - Access sensitive documents
        - Move laterally across the network
        - Install backdoors or malware

Potential Impact:

Successful exploitation of CVE-2026-20963 may allow attackers to:

- Execute arbitrary code on SharePoint servers
- Fully compromise confidentiality, integrity, and availability
- Access or exfiltrate sensitive organizational data

- Modify or delete documents and system content
- Use the compromised server for lateral movement within the network

Because SharePoint often stores critical internal documents and operational data, impact can extend beyond the server to the entire enterprise environment.

Mitigation process

CERTVU recommends the following:

Apply Microsoft Security Updates (Critical)

- Install the latest SharePoint security patches provided by Microsoft immediately.
- Ensure all SharePoint servers are updated to patched build versions**.**

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-20963

.