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

17 July 2026

Advisory 170: Microsoft SharePoint Deserialization of Untrusted Data Vulnerability

Release Date: 16th July 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?

CVE-2026-58644 is a remote code execution flaw caused by the deserialization of untrusted data that allows an unauthenticated threat actor to execute code remotely on a vulnerable SharePoint Server.

The vulnerability is a critical RCE vulnerability affecting Microsoft SharePoint Server with a CVSS score of 9.8. It stems from a deserialization of untrusted data flaw (CWE-502) and is remotely exploitable with low attack complexity.

What are the systems affected?

In a network-based attack, an attacker authenticated as at least a Site Owner could inject and execute arbitrary code remotely on the SharePoint Server. However, per the NVD record and multiple vendor analyses, CVE-2026-58644 is exploitable by unauthenticated attackers — no account is required.

Microsoft SharePoint Server 2016 – Affected

Microsoft SharePoint Enterprise Server 2016 – Affected
Microsoft SharePoint Server 2019 – Affected
Microsoft SharePoint Server Subscription Edition – Affected
Microsoft SharePoint Online (M365 cloud) – Patched automatically

What does this mean?

Both vulnerabilities stem from deserialization of untrusted data flaws and are remotely exploitable with low attack complexity.

Step 1 - Reconnaissance
The attacker identifies internet-facing SharePoint Server deployments running unpatched versions. SharePoint servers are commonly internet-accessible for collaboration and document management purposes.

Step 2 - Crafted Serialized Object
The exploitation of this vulnerability involves sending a crafted serialized .NET object to a vulnerable SharePoint endpoint. The attacker crafts a malicious .NET object designed to execute arbitrary code when deserialized by the SharePoint application.

Step 3 - Unauthenticated HTTP Request
The attacker delivers the crafted serialized payload via a specially crafted HTTP request to the vulnerable SharePoint endpoint. No authentication, no credentials, and no user interaction are required - the attack is fully remote and automated.

Step 4 - Deserialization Triggers Code Execution
SharePoint deserializes the untrusted object without adequate validation. The deserialization process instantiates the attacker's malicious .NET object, executing arbitrary code in the context of the SharePoint application pool - typically running under a highly privileged service account.

Mitigation process

CERTVU recommends the following:

Apply July 2026 Security Update Immediately

Install the July 14, 2026 Patch Tuesday cumulative update for your SharePoint Server version:

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-58644

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-58644
3. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-58644