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

27 July 2026

Advisory 173: Microsoft SharePoint Server Deserialization of Untrusted Data Vulnerability (CVE-2026-50522).

Release Date: 24th 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?

Microsoft SharePoint Server contains a deserialization of untrusted data vulnerability (CWE-502) that allows an unauthenticated attacker to execute arbitrary code over a network, with no user interaction required. The vulnerability carries a CVSS v3.1 base score of 9.8 (Critical), and Microsoft has assessed it as "Exploitation More Likely."

A working exploit for this vulnerability was first demonstrated at Pwn2Own Berlin and provided to Microsoft ahead of a fix. Despite this responsible disclosure, active in-the-wild exploitation only began after a public proof-of-concept was released on 20 July 2026, with successful attacks against internet-facing, unpatched on-premises SharePoint servers observed within hours. CVE-2026-50522 is the fourth SharePoint Server vulnerability confirmed under active exploitation in the current wave, alongside CVE-2026-32201 (addressed in CERTVU Advisory 137), CVE-2026-45659, CVE-2026-56164 and CVE-2026-58644.

What are the systems affected?

The vulnerability affects the following on-premises Microsoft products (this does not affect SharePoint Online / Microsoft 365):

- Microsoft SharePoint Enterprise Server 2016 (x64-based System)
  - Version affected: builds earlier than 16.0.5561.1001
- Microsoft SharePoint Server 2019 (x64-based System)
  - Version affected: builds earlier than 16.0.10417.20175
- Microsoft SharePoint Server Subscription Edition (x64-based System)
  - Version affected: builds earlier than 16.0.19725.20434

What does this mean?

Exploitation is network-based, requires no authentication, and requires no user interaction.

Typical attack flow:

1. Target identification
   - Attacker locates internet-facing or internally exposed on-premises SharePoint servers.
2. Malicious sign-in request
   - A crafted WS-Federation sign-in response containing a forged SecurityContextToken is submitted to the SharePoint /_trust/default endpoint.
3. Deserialization and code execution
   - The token's cookie value carries a malicious .NET BinaryFormatter payload. SharePoint deserializes it without validating authenticity, executing attacker-supplied code in the context of the IIS worker process (w3wp.exe).
4. Machine key theft
   - With code execution established, attackers extract the server's IIS machine keys (validationKey and decryptionKey) from web.config in a single follow-up request.
5. Persistent, re-authenticated access
   - Using the stolen machine keys, attackers can forge valid authentication tokens (e.g. ViewState/session tokens) and regain access to the server even after the underlying vulnerability has been patched, unless the keys themselves are also rotated.

Mitigation process

CERTVU recommends the following:

- Apply Microsoft's July 2026 security update for CVE-2026-50522 immediately across all on-premises SharePoint farm servers (Enterprise Server 2016, Server 2019, Subscription Edition). This vulnerability is listed on the CISA Known Exploited Vulnerabilities (KEV) catalog (added 22 July 2026, federal remediation due date 25 July 2026).
- Patching alone is not sufficient. Any SharePoint server that was internet-facing or otherwise exposed before patching should have its IIS machine keys (validationKey and decryptionKey) rotated, per Microsoft's guidance, since a stolen machine key survives the patch.
- Review IIS and SharePoint ULS logs for requests to the /_trust/default endpoint and for anomalous child processes spawned by w3wp.exe, which may indicate prior exploitation.

- Restrict direct internet exposure of on-premises SharePoint servers where feasible, and apply network segmentation or WAF rules pending confirmation that all farm servers are patched.
- Confirm patch status against the full current SharePoint exploitation wave - CVE-2026-32201 (CERTVU Advisory 137), CVE-2026-45659, CVE-2026-56164 and CVE-2026-58644 - not this CVE in isolation.

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-50522
3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50522
4. https://cwe.mitre.org/data/definitions/502.html
5. https://www.cisa.gov/news-events/alerts/2026/07/14/cisa-urges-sharepoint-hardening-after-new-exploitations