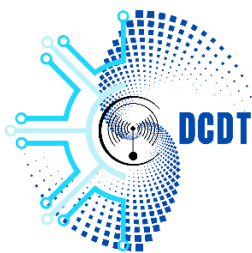


**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

15 July 2026

Advisory 167: CVE-2026-56164_Microsoft SharePoint Server Missing Authentication for Critical Function Vulnerability

Release Date: 14th 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-2026-56164 is a SharePoint Server flaw that Microsoft says is being exploited in attacks. It lets an unauthenticated attacker escalate privileges over the network — no credentials, no user interaction, remote.

What are the systems affected?

CVE-2026-56164 affects Microsoft SharePoint Server 2019, Microsoft SharePoint Server Subscription Edition, as well as SharePoint Server 2016 and SharePoint Enterprise Server 2016.

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) - (Patched automatically)

What does this mean?

CVE-2026-56164 presents an operational risk because it affects Microsoft SharePoint Server and can be exploited over a network. Microsoft attributes the vulnerability to missing authentication for a critical function, allowing an unauthorized attacker to gain elevated privileges.

Step 1 — Reconnaissance

The attacker identifies an organization running an on-premises SharePoint Server deployment accessible over the network. SharePoint farms are commonly internet-facing or accessible from within a corporate network.

Step 2 — Unauthenticated Network Request

The attacker escalates privileges over the network with no credentials and no user interaction required — purely remote. The missing authentication check on a critical SharePoint function allows the attacker to submit a crafted request without first authenticating.

Step 3 — Privilege Escalation

The crafted request exploits the missing authentication gate to gain elevated privileges on the SharePoint Server — moving from unauthenticated access to a privileged position within the SharePoint environment.

Step 4 — Chaining for Full Compromise

CVE-2026-56164 targets Microsoft SharePoint Server and allows an attacker to escalate privileges on a compromised or authenticated session, a pattern consistent with prior SharePoint EoP flaws that have been chained with RCE bugs for full server takeover.

Mitigation process

CERTVU recommends the following:

Primary - Apply July 2026 Security Update Immediately

Install Microsoft's July 14, 2026 Patch Tuesday security update for your SharePoint Server version. Obtain updates from the Microsoft Security Update Guide:

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-56164>

SharePoint Server 2016	July 2026 cumulative update
SharePoint Enterprise Server 2016	July 2026 cumulative update
SharePoint Server 2019	July 2026 cumulative update
SharePoint Subscription Edition	July 2026 cumulative update

Reference

1. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
2. <https://www.cve.org/CVERecord?id=CVE-2026-56164>
3. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-56164>

