**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

19 August 2026

**Advisory 192: CVE-2026-55040_Microsoft SharePoint Weak Authentication Vulnerability**

**Release Date:** 14th July 2026 (Added 19 August 2026)
**Impact:** 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-2026-55040 is a critical-severity authentication bypass vulnerability in on-premises Microsoft SharePoint Server. It carries a CVSS Base Score of 9.1 and is caused by a chain of four distinct weaknesses in SharePoint's JSON Web Token (JWT) validation pipeline (CWE-1390). A remote, unauthenticated attacker can forge a valid JWT and impersonate any SharePoint site user or administrator, with no credentials, prior access, or user interaction required.

# What are the systems affected?

Affected systems are limited to on-premises SharePoint deployments; SharePoint Online (Microsoft 365) is not affected by this vulnerability.

Microsoft SharePoint Enterprise Server 2016 – (Affected)
Microsoft SharePoint Server 2019 – (Affected)
Microsoft SharePoint Server Subscription Edition – (Affected)

SharePoint Online (Microsoft 365) – (Not affected)

Any organisation running on-premises SharePoint for intranets, document management, or workflow automation faces critical risk, given confirmed active exploitation and a publicly available proof-of-concept exploit.

# What does this mean?

This flaw requires no initial access step at all: the attacker needs only network reachability to a vulnerable SharePoint server and the identity they wish to impersonate.

**Step 1 - Target Identity Discovery**
The attacker identifies a user to impersonate using a Windows Security Identifier (SID) or User Principal Name (UPN). SIDs can be enumerated over SMB; UPNs commonly resemble an email address and can be guessed, harvested, or derived from the server's own certificate.

**Step 2 - Exploiting the JWT Validation Chain**
Four separate weaknesses combine to defeat token validation: the signature check accepts any non-empty string rather than a genuine cryptographic signature, and the issuer check passes because the attacker's forged certificate is never compared against the actual trusted issuer list.

**Step 3 - JWT Forgery and Impersonation**
The attacker forges a JWT asserting the chosen identity. SharePoint accepts the forged token as legitimate and grants a session with that user's full permissions, including administrator rights if an administrator account was targeted.

**Step 4 - Chaining to Full Remote Code Execution**
Rapid7 has demonstrated that this authentication bypass can be chained with **CVE-2026-63520**, patched in Microsoft's August 2026 release, to achieve full unauthenticated remote code execution on the underlying server - installing CVE-2026-55040's July fix alone already breaks this chain.

# Mitigation process

CERTVU recommends the following:

1. **Apply the July and August 2026 Security Updates**

Install the 14 July 2026 SharePoint security update that addresses CVE-2026-55040 on every on-premises farm server, then complete the SharePoint configuration wizard on each server and verify the resulting build number. Given a public proof-of-concept exploit is now available and active exploitation has been observed, treat any unpatched, internet-reachable SharePoint server as an emergency. Also apply Microsoft's August 2026 update addressing CVE-2026-63520, since the two vulnerabilities can be chained into full unauthenticated remote code execution.

*Rapid7 Technical Analysis: CVE-2026-55040*

# Reference


1. https://www.cisa.gov/news-events/alerts/2026/07/14/cisa-urges-sharepoint-hardening-after-new-exploitations
2. https://www.cve.org/CVERecord?id=CVE-2026-55040
3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55040


.