مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Critical Remote Code Execution Vulnerability in Microsoft SharePoint Online

Tracking #:432318049

Date:21-11-2025



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Microsoft has published a critical security advisory for CVE-2025-59245, a Remote Code Execution (RCE) vulnerability impacting SharePoint Online.

## TECHNICAL DETAILS:

Microsoft has published a Critical security advisory for CVE-2025-59245, a Remote Code Execution (RCE) vulnerability impacting SharePoint Online, stemming from CWE-502: Deserialization of Untrusted Data. The vulnerability received a CVSS v3.1 base score of 9.8, indicating a high-impact, low-complexity threat capable of remote, unauthenticated exploitation.

Microsoft confirms that this vulnerability has been fully mitigated within the SharePoint Online service, and therefore no customer action is required. The CVE was published as part of Microsoft's initiative to improve transparency for cloud-service vulnerabilities.
There is no evidence of public disclosure or active exploitation, and no exploit code is currently available.

**Vulnerability Details:**

- CVE-2025-59245
- CVSS:3.1 9.8,Critical
- The vulnerability arises from unsafe deserialization of untrusted data within Microsoft SharePoint Online. Successful exploitation could allow a remote attacker to execute arbitrary code in the context of the SharePoint Online service.

## RECOMMENDATIONS:

- No action is required for SharePoint Online, but on-premises deployments should ensure all updates are applied.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-59245