



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates - Microsoft
Tracking #:432318952
Date:13-05-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Microsoft has released security updates to patch multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Microsoft has released its May 2026 Security Updates to address multiple vulnerabilities, including several critical vulnerabilities affecting Azure, Windows, SharePoint, Dynamics 365, Azure DevOps, Hyper-V, and enterprise cloud services. Successful exploitation could allow remote code execution (RCE), privilege escalation, spoofing, information disclosure, or complete system compromise across enterprise environments.

Vulnerability Details

Critical Vulnerabilities

- **CVE-2026-42826** – Azure DevOps Information Disclosure Vulnerability
- **CVE-2026-33109** – Azure Managed Instance for Apache Cassandra Remote Code Execution Vulnerability.
- **CVE-2026-42823** – Azure Logic Apps Elevation of Privilege Vulnerability.
- **CVE-2026-42898** – Microsoft Dynamics 365 On-Premises Remote Code Execution Vulnerability.
- **CVE-2026-41089** – Windows Netlogon Remote Code Execution Vulnerability.
- **CVE-2026-41096** – Windows DNS Client Remote Code Execution Vulnerability.
- **CVE-2026-33823** – Microsoft Team Events Portal Information Disclosure Vulnerability.
- **CVE-2026-35428** – Azure Cloud Shell Spoofing Vulnerability.
- **CVE-2026-40379** – Microsoft Enterprise Security Token Service (ESTS) Spoofing Vulnerability.
- **CVE-2026-40402** – Windows Hyper-V Elevation of Privilege Vulnerability.
- **CVE-2026-33117** – Azure SDK for Java Security Feature Bypass Vulnerability.
- **CVE-2026-41103** – Microsoft SSO Plugin for Jira & Confluence Elevation of Privilege Vulnerability.
- **CVE-2026-42833** – Microsoft Dynamics 365 On-Premises Remote Code Execution Vulnerability.
- **CVE-2026-33844** – Azure Managed Instance for Apache Cassandra Remote Code Execution Vulnerability.

Other Notable Vulnerabilities:

- CVE-2026-35421 - Windows GDI Remote Code Execution Vulnerability
- SharePoint (Multiple CVEs including CVE-2026-33110, 33112, 35439, 40357, 40365) – Multiple remote code execution vulnerabilities.

Note: Refer to the Microsoft May 2026 release notes for the full list of CVEs and additional information.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Microsoft.

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/releaseNote/2026-may>