مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates- Microsoft

Tracking #:432315855

Date:15-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council observed that Microsoft released Patch Tuesday's May 2024 updates addressing several vulnerabilities including Zero days.

TECHNICAL DETAILS:

Microsoft Patch Tuesday's May 2024 edition addressed 67 vulnerabilities, including one critical and 59 important severity vulnerabilities. In this month's security updates, Microsoft has addressed **two zero-day vulnerabilities known to be exploited in the wild.**

Actively exploited Vulnerabilities:

- **CVE-2024-30051:Microsoft DWM Core Library Privilege Escalation Vulnerability** This privilege escalation vulnerability allows an attacker to gain SYSTEM privileges.

- **CVE-2024-30040- Microsoft Windows MSHTML Platform Security Feature Bypass Vulnerability.** Microsoft Windows MSHTML Platform contains an unspecified vulnerability that allows for a security feature bypass.

Critical Vulnerability:

- **CVE-2024-30044-Microsoft SharePoint Server Remote Code Execution Vulnerability.** An authenticated attacker with Site Owner permissions or higher could upload a specially crafted file to the targeted Sharepoint Server and craft specialized API requests to trigger deserialization of file's parameters. This would enable the attacker to perform remote code execution in the context of the Sharepoint Server.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to apply the latest security updates and Prioritize Zero-Day Patches.

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/2024-May