



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates- Microsoft Edge Browser

Tracking #:432316137

Date:12-08-2024

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 observed that Microsoft released security updates to patch multiple vulnerabilities in the Edge browser.

TECHNICAL DETAILS:

Microsoft has released security updates to address two vulnerabilities affecting Microsoft Edge. These vulnerabilities could potentially allow remote code execution (RCE) and memory corruption, leading to a compromise of the affected system.

Vulnerabilities Details:

- **CVE-2024-38219**
 - CVSS Score 6.5 Medium
 - A remote code execution vulnerability exists in Microsoft Edge (Chromium-based). Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code in the context of the current user.
- **CVE-2024-38218**
 - CVSS Score 8.4 High
 - Memory corruption vulnerability exists in Microsoft Edge (HTML-based). Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code in the context of the current user.

Fixed Versions:

- Microsoft Edge Stable Channel (Version 127.0.2651.98)
- Microsoft Edge Extended Stable Channel (Version 126.0.2592.137)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update the Microsoft Edge browser to the latest version.

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://learn.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security>