مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Microsoft Security Updates

Tracking #:432316036

Date:10-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Microsoft recently released security updates to patch multiple vulnerabilities across various products.

TECHNICAL DETAILS:

Microsoft released security updates to address multiple vulnerabilities across various products. These updates address a substantial number of vulnerabilities (139) across various products, including Windows, Office, .NET, Azure, and more. **Some of these were critical and actively exploited.**

Notable Vulnerabilities Details:

Actively Exploited:

- **CVE-2024-38080-**Microsoft Windows Hyper-V Privilege Escalation Vulnerability
- **CVE-2024-38112**-Microsoft Windows MSHTML Platform Spoofing Vulnerability

Critical:

- **CVE-2024-38074, CVE-2024-38076,CVE-2024-38077 CVSS Score:9.8 Critical-** Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability
- **CVE-2024-38089**- **CVSS Score:9.1 Critical**-Microsoft Defender for IoT Elevation of Privilege Vulnerability

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to prioritize patches for the Critical and Actively exploited vulnerabilities at the earliest and Install other updates.

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-Jul