مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploited Vulnerabilities in Microsoft Products

Tracking #:432315668

Date:05-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Microsoft products that are being actively exploited by threat actors to gain unauthorized access and complete control of affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

1.CVE-2024-21338

- CVSS Base Score: 7.8 HIGH
- A vulnerability in the Microsoft Windows kernel, related to insufficient access control within the IOCTL dispatcher (appid.sys), allows local attackers to escalate privileges to SYSTEM level. Successful exploitation could grant attackers complete control over the affected system.
- Note: According to reports, this vulnerability was exploited by the Lazarus hacker group in attacks involving the FudModule rootkit

2.CVE-2023-29360

- CVSS Base Score: 8.4 HIGH
- Microsoft Streaming Service contains an untrusted pointer dereference vulnerability, which allows local attackers to escalate privileges to SYSTEM level.
- Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code or cause a denial-of-service condition on the affected system.

Affected Products:
Windows 10 and 11 and Windows Server 2016, 2019, and 2022

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/vulnerability/CVE-2024-21338
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29360