مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in Microsoft Defender Antimalware Platform

Tracking #:432318834

Date:23-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity Elevation of Privilege (EoP) vulnerability affecting the Microsoft Defender Antimalware Platform is now actively exploited in the wild.

TECHNICAL DETAILS:

A high-severity Elevation of Privilege (EoP) vulnerability affecting the Microsoft Defender Antimalware Platform is now actively exploited in the wild. The flaw stems from insufficient granularity of access control and allows a low-privileged local attacker to escalate privileges to SYSTEM level, potentially leading to full system compromise.

Vulnerability Details

- CVE ID: CVE-2026-33825
- Type: Elevation of Privilege (EoP)
- CWE: CWE-1220 – Insufficient Granularity of Access Control
- CVSS v3.1 Score: 7.8 (High)
- Attack Vector: Local
- Privileges Required: Low
- User Interaction: None
- Attack Complexity: Low

Exploitation Status

- Actively Exploited: Yes

Affected Products

- Product: Microsoft Defender Antimalware Platform
- Affected Versions:
  - Versions prior to 4.18.26030.3011
- Patched Version:
  - 4.18.26030.3011 and later

RECOMMENDATIONS:

Immediate Actions

- Update Microsoft Defender to fixed version or later.
- Verify that updates are successfully deployed across all systems.

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-2026-33825