NATIONAL CSIRT-CY

Actively Exploited Vulnerability in **Microsoft Defender Antimalware Platform**

23 April 2026

[Cyber Threat Intelligence]

EXECUTIVE SUMMARY:

The Digital Security Authority (DSA) 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

Exploitation Status

- Product: Microsoft Defender Antimalware Platform
- Affected 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.

Please ensure to distribute this information among your subsidiaries and partners and provide us with any pertinent information or findings you may have (such as Indicators of Compromise, Tactics, Techniques, and Procedures, etc.).

The Digital Security Authority (DSA) extends its appreciation for the continued collaboration.

REFERENCES:

1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825

DISCLAIMER:

The information presented in this report is based on available data up to the 23rd of April 2026.

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.