مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Microsoft Defender 'RoguePlanet' Privilege Escalation Vulnerability

Tracking #:432319288

Date:13-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Microsoft has released an out-of-band security update to address, a High-severity Elevation of Privilege (EoP) vulnerability affecting the Microsoft Malware Protection Engine used by Microsoft Defender Antivirus.

TECHNICAL DETAILS:

Microsoft has released an out-of-band security update to address CVE-2026-50656, a High-severity Elevation of Privilege (EoP) vulnerability affecting the Microsoft Malware Protection Engine (mpengine.dll) used by Microsoft Defender Antivirus. he vulnerability, publicly known as "RoguePlanet," allows a local attacker with standard user privileges to escalate to NT AUTHORITY\SYSTEM, providing complete control over the affected Windows system.
The vulnerability exploits a race condition within the Microsoft Malware Protection Engine. Public proof-of-concept (PoC) exploit code was released in June 2026 by security researcher Nightmare-Eclipse, increasing the likelihood of exploitation despite the absence of confirmed in-the-wild attacks. Microsoft addressed the issue by releasing Microsoft Malware Protection Engine version 1.1.26060.3008, which is distributed automatically through Microsoft Defender updates.

Vulnerability Details:

- CVE ID: CVE-2026-50656
- Vulnerability Name: RoguePlanet
- Severity: High
- CVSS Score: 7.8
- Vulnerability Type: Elevation of Privilege (Local Privilege Escalation)
- CWE: CWE-362 – Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
- Fixed Version: Microsoft Malware Protection Engine 1.1.26060.3008 or later.

RECOMMENDATIONS:

Immediate Actions:

- Verify Microsoft Defender Engine Version: Ensure all Windows endpoints are running Microsoft Malware Protection Engine version 1.1.26060.3008 or later. Although the engine updates automatically through Microsoft Defender, administrators should verify successful deployment using the Microsoft Defender portal, Microsoft Defender for Endpoint, or PowerShell to confirm all systems are protected.

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-2026-50656