

HiveForce Labs

THREAT ADVISORY

 VULNERABILITY REPORT

RoguePlanet: A Defender Race Condition That Opens a Direct Path to SYSTEM

Date of Publication

July 10, 2026

Admiralty Code

A1

TA Number

TA2026195

Summary

First Seen: June 16, 2026

Affected Products: Microsoft Defender

Impact: Microsoft Defender has a flaw nicknamed RoguePlanet (CVE-2026-50656) that turned the security tool itself into an attacker's foothold. It's a race condition in Defender's scanning engine, meaning an attacker who's already on a machine can win a split-second timing gap to pop open a command prompt with SYSTEM access, the highest level on Windows. The catch (or the scary part): it worked on fully patched Windows 10 and 11, and whether or not real-time protection was switched on. A researcher went public with a working proof-of-concept during a spat with Microsoft over its bug-bounty practices. No known threat group or malware has been tied to it, and Microsoft has since fixed it in Malware Protection Engine version 1.1.26060.3008.

CVE

CVE	NAME	AFFECTED PRODUCT	ZER O- DAY	CISA KEV	PATC H
CVE-2026-50656	RoguePlanet (Microsoft Defender Privilege Escalation Vulnerability)	Microsoft Defender			

Vulnerability Details

#1

CVE-2026-50656, nicknamed RoguePlanet, is an elevation-of-privilege vulnerability. It sits in the Microsoft Malware Protection Engine, the component that provides scanning, detection, and cleaning for Microsoft Defender and related antimalware products.

#2

The root cause is a timing flaw: the engine performs an operation in a way that can be interrupted and manipulated in the narrow gap between a check and the action that follows it. An attacker who can already run code locally races the engine to win that window and redirect a privileged operation, which ends with a shell running as SYSTEM.

#3

The researcher confirmed it works with protection on or off, and possibly in passive mode. Once SYSTEM access is obtained, the attacker can execute arbitrary code and carry out unauthorized actions at the highest privilege level Windows offers.

#4

The flaw affects Microsoft Defender's Malware Protection Engine across supported Windows 10 and Windows 11 builds, and the public exploit was demonstrated working on systems that already had the June 2026 Patch Tuesday updates installed, meaning "fully patched" machines remained exposed until the engine itself was updated.

#5

A working proof-of-concept exploit for RoguePlanet has been made public. The flaw was disclosed in June, but Microsoft released the fix this month, updating the Microsoft Malware Protection Engine to address the vulnerability.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-50656	Microsoft Defender – Malware Protection Engine (Before 1.1.26060.3008)	cpe:2.3:a:microsoft:malware_protection_engine:-:*:*:*:*:*	CWE-59

Recommendations

- 

Confirm the Engine Update Is Installed: Verify that the Microsoft Malware Protection Engine is at version 1.1.26060.3008 or later, which contains the fix. Check the engine version in the Windows Security app or through your endpoint management tooling, and trigger a manual definition/engine update on any machine that has been offline.
- 

Let Automatic Updates Run, but Verify Coverage: Microsoft states no user action is normally required because the engine updates automatically, often several times a day when connected to the internet. Still, confirm that endpoints, servers, and isolated or air-gapped systems are actually receiving engine updates, since those hosts are the most likely to lag behind.
- 

Enforce Least Privilege and Limit Local Code Execution: Because this is a local escalation flaw, an attacker needs an initial foothold to use it. Restrict who can run code on endpoints, apply application control or allow-listing, and reduce standing local-admin rights so an initial compromise has fewer paths to escalate.
- 

Watch for Unexpected SYSTEM Shells: Monitor for command interpreters such as cmd.exe or powershell.exe spawning as SYSTEM from unusual parent processes, particularly those tied to the antimalware engine. A sudden SYSTEM-level shell with no legitimate administrative context is a strong signal worth investigating.



Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Execution	<u>T1059</u> : Command and Scripting Interpreter	
Privilege Escalation	<u>T1068</u> : Exploitation for Privilege Escalation	
Resource Development	<u>T1588</u> : Obtain Capabilities	<u>T1588.006</u> : Vulnerabilities



Patch Link

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2026-50656>



References

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2026-50656>

<https://blog.projectnightcrawler.dev/posts/2026-06-16-rogueplanet-another-quick-statement/>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of HivePro.

REPORT GENERATED ON

July 10, 2026 • 09:00 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com