UPDATE: Microsoft Releases Fix for RoguePlanet Microsoft Malware Protection Engine Privilege Escalation Vulnerability

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

A new proof-of-concept exploit called ShieldBreak may bypass Microsoft's fix for CVE-2026-50656, also known as RoguePlanet.

Organizations should continue using Microsoft Malware Protection Engine version 1.1.26060.3008 or later to block the original exploit, but that version does not provide confirmed protection against ShieldBreak.

Update – 8/13/2026
New Exploit May Bypass Microsoft's RoguePlanet Fix

The original Aspire CTI Emergency Flash Notice reported that Microsoft fixed CVE-2026-50656 by releasing Malware Protection Engine version 1.1.26060.3008. Organizations were advised to verify that Defender had been updated to that version or later.

On August 12, 2026, the same researcher who disclosed RoguePlanet released ShieldBreak. The researcher describes it as a full bypass of Microsoft's fix for CVE-2026-50656. Independent security researchers have confirmed that ShieldBreak works on updated Windows 11 systems.

Updated Affected Products

The original notice identified Windows 10 and Windows 11 as affected by RoguePlanet. The ShieldBreak proof-of-concept has now been tested on:

- Windows 11 25H2
- Windows 11 Canary builds
- Windows Server 2025

The original RoguePlanet exploit used a file-system race condition to manipulate Microsoft Defender's quarantine process. ShieldBreak reaches the same result through a different method. It changes file contents while Defender performs a cloud-based scan, causing Defender to write an attacker-controlled `phoneinfo.dll` file to the Windows System32 directory. The exploit then triggers a Windows Error Reporting task that loads the DLL and opens a command shell with SYSTEM privileges.

The researcher also states that Windows 10 and corresponding Windows Server editions are vulnerable, but the released proof-of-concept does not currently support those systems. This changes the guidance in the original notice. Organizations should still install version 1.1.26060.3008 or later because it blocks the original RoguePlanet exploit. However, installing that update does not currently provide confirmed protection against ShieldBreak.

The researcher who disclosed RoguePlanet says ShieldBreak fully bypasses Microsoft's patch. Microsoft has not confirmed that claim and is investigating whether ShieldBreak bypasses CVE-2026-50656 or is a separate vulnerability. No fix is currently available, and there is no evidence of active exploitation. Aspire's CTI team will update this notice as more details become available.

Updated Aspire Protects

- Continue using Microsoft Malware Protection Engine version 1.1.26060.3008 or later for CVE-2026-50656. Do not consider the engine version alone proof that an endpoint is protected from ShieldBreak.
- Monitor for C:\Windows\System32\phoneinfo.dll and directories beginning with C:\ShieldBreak_.
- Investigate wermgr.exe -upload activity followed by conhost.exe running with SYSTEM privileges.
- Block unapproved applications from running on endpoints.

Updated IoCs

There are no known network-based IoCs. The following host artifacts are associated with the public ShieldBreak proof-of-concept:

- C:\ShieldBreak_<GUID>
- C:\Windows\System32\phoneinfo.dll
- WD_SHADOW_<GUID>
- WD_TARGET_<GUID>
- wermgr.exe -upload followed by a SYSTEM-level conhost.exe process

Overview

There is a high-severity vulnerability (CVE-2026-50656, CVSS 7.8) in the Microsoft Malware Protection Engine used by Microsoft Defender on Windows 10 and Windows 11 systems. The vulnerability is caused by improper link resolution before file access and may allow an authenticated attacker to elevate privileges to SYSTEM through a low-complexity attack.

Affected Products

- Microsoft Malware Protection Engine versions prior to 1.1.26060.3008
- Windows 10
- Windows 11

CVE-2026-50656 was publicly disclosed in June after proof-of-concept exploit code was released by the researcher known as Nightmare Eclipse. Microsoft addressed the vulnerability by releasing Microsoft Malware Protection Engine version 1.1.26060.3008.

Although Microsoft states the vulnerability is not currently being actively exploited, the company has assessed that exploitation is more likely because a public exploit is available. Systems configured to receive Defender engine updates automatically should receive the fix without additional action. Organizations that manage updates manually should confirm the updated engine has been installed across affected endpoints.

Aspire Protects

- **Patch** - Verify Microsoft Malware Protection Engine has been updated to version 1.1.26060.3008 or later.
- Ensure Microsoft Defender engine and security intelligence updates are configured to install automatically whenever possible.
- If automatic updates are disabled or managed internally, manually deploy the latest Microsoft Malware Protection Engine update.
- Review endpoint management tools to confirm all Windows 10 and Windows 11 systems have received the updated engine.

TTPs to Watch

Privilege Escalation

- Exploitation for Privilege Escalation (T1068) – An attacker may exploit the vulnerability to obtain SYSTEM privileges on a vulnerable Windows system.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Organizations running Microsoft Defender on Windows 10 or Windows 11 systems may be affected, particularly enterprise environments that centrally manage endpoint protection.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will

ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

- Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

CVE-2026-50656 - Security Update Guide - Microsoft - Microsoft Defender Elevation of Privilege Vulnerability

ThreatHunting/AdvancedHuntingQueries/ShieldBreak.kql at master · GossiTheDog/ThreatHunting · GitHub

CVE-2026-50656 ShieldBreak Claims Defender Fix Bypass