Microsoft Defender Zero-Day Vulnerabilities Actively Exploited in the Wild

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

TL;DR

Microsoft Defender has two actively exploited vulnerabilities affecting separate Defender components. CVE-2026-41091 (CVSS 7.8) impacts the Microsoft Malware Protection Engine and may allow a threat actor to gain SYSTEM privileges on a device.

CVE-2026-45498 (CVSS 4.0) impacts Microsoft Defender Antimalware Platform and may cause affected systems to become unstable or unavailable. Microsoft released fixes for both vulnerabilities.

Overview

There are two actively exploited vulnerabilities affecting Microsoft Defender components used across Windows environments.

CVE-2026-41091 (CVSS 7.8) is an elevation of privilege vulnerability affecting the Microsoft Malware Protection Engine. The vulnerability is caused by improper link resolution before file access, also known as a link following flaw. According to Microsoft, a successful attacker may gain SYSTEM privileges on the affected device.

CVE-2026-45498 (CVSS 4) is a denial-of-service vulnerability affecting Microsoft Defender Antimalware Platform. Microsoft stated successful exploitation may allow a threat actor to cause denial-of-service conditions on vulnerable Windows systems.

Affected Products

- Microsoft Malware Protection Engine version 1.1.26030.3008 and earlier
- Microsoft Defender Antimalware Platform version 4.18.26030.3011 and earlier

Microsoft confirmed both vulnerabilities are being exploited in the wild. If exploited, a threat actor could gain SYSTEM-level access to a Windows device or interfere with Microsoft Defender protections across the environment. In large Windows deployments, that could allow attackers to move through systems more freely while security teams lose visibility into activity taking place on affected endpoints.

Aspire Protects

- **Patch** - Update Microsoft Malware Protection Engine and Microsoft Defender Antimalware Platform to the latest versions.
- Verify Microsoft Defender automatic updates are functioning correctly across all endpoints.

- Monitor for unusual privilege escalation behavior or Defender-related service instability.
- Confirm endpoint protection platforms are receiving current engine and signature updates.

TTPs to Watch

Privilege Escalation

- Abuse Elevation Control Mechanism [T1548] – The attacker may exploit improper link resolution behavior in CVE-2026-41091 to gain SYSTEM privileges on a Windows device.

Impact

- Endpoint Denial of Service [T1499] – The attacker may exploit CVE-2026-45498 to disrupt the availability or stability of affected Windows systems.

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

The Microsoft Defender vulnerabilities threaten any organization using Windows endpoints protected by Microsoft Defender.

- 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-2026-45498 - Security Update Guide - Microsoft - Microsoft Defender Denial of Service Vulnerability

CVE-2026-41091 - Security Update Guide - Microsoft - Microsoft Defender Elevation of Privilege Vulnerability