

Forum:[Hack Forums](#)

Thread: [Microsoft Warns of Two Actively Exploited Defender Vulnerabilities](#)

MadScientist - May 23, 2026, 2:34 am

Microsoft has disclosed that a privilege escalation and a denial-of-service flaw in Defender has come under active exploitation in the wild.

The former, tracked as CVE-2026-41091, is rated 7.8 on the CVSS scoring system. Successful exploitation of the flaw could allow an attacker to gain SYSTEM privileges.

"Improper link resolution before file access ('link following') in Microsoft Defender allows an authorized attacker to elevate privileges locally," Microsoft said in an advisory.

The second vulnerability under exploitation is CVE-2026-45498 (CVSS score: 4.0), a denial-of-service bug impacting Defender. The two vulnerabilities have been addressed in Microsoft Defender Antimalware Platform versions 1.1.26040.8 and 4.18.26040.7, respectively.

Although Microsoft has not formally confirmed, the vulnerability descriptions for CVE-2026-41091 and CVE-2026-45498 overlap with that of RedSun and UnDefend, two Defender zero-days that were disclosed by Chaotic Eclipse (aka Nightmare-Eclipse) last month. Huntress has since observed exploitation of both the vulnerabilities, alongside BlueHammer (CVE-2026-33825).

Also addressed in version 1.1.26040.8 is a heap-based buffer overflow vulnerability in Defender (CVE-2026-45584, CVSS score: 8.1) that an unauthorized attacker could exploit to achieve remote code execution. There is no evidence the vulnerability has been exploited in the wild.

Read More - <https://thehackernews.com/2026/05/microsoft-warns-of-two-actively.html>

loadman - May 23, 2026, 2:42 am

<https://github.com/Nightmare-Eclipse/>

sadly github got taken down

MadScientist - May 23, 2026, 3:01 am

(May 23, 2026 02:42 AM)loadman Wrote: [\[CITE\] https://github.com/Nightmare-Eclipse/](#)

sadly github got taken down

Yeah that's a shame, I would have loved to back it up

Mastercarder - May 23, 2026, 4:10 am

Interesting seeing Defender get hit this hard lately. A lot of people treat antivirus like an untouchable security layer, but once something gets SYSTEM privileges it's basically game over on that machine.

The scary part isn't even the DoS bug, it's the privilege escalation being actively exploited in the wild already. Goes to show even security software itself becomes an attack surface eventually.