Microsoft Defender "RedSun" Zero-Day and "UnDefend" Tool Allow SYSTEM Access and Disable Security Protections

TL;DR

New Microsoft Defender zero-day activity includes the RedSun exploit, which allows attackers to gain SYSTEM privileges on fully patched Windows systems, and a separate tool called UnDefend, which can block security updates or disrupt Defender functionality without administrative privileges.

This activity follows the recently patched BlueHammer vulnerability (CVE-2026-33825, CVSS 7.8). RedSun and UnDefend remain unpatched and are being exploited in the wild.

Overview

There is ongoing exploitation of multiple Microsoft Defender weaknesses, including a zero-day known as "RedSun" and a separate tool referred to as "UnDefend". These issues impact Windows 10, Windows 11, and Windows Server systems, even when fully updated.

Affected Products

- Microsoft Defender (enabled environments)
- Windows 10
- Windows 11
- Windows Server 2019 and later

This activity follows the earlier "BlueHammer" vulnerability (CVE-2026-33825, CVSS 7.8), which Microsoft patched during April 2026 updates. BlueHammer allowed attackers to escalate privileges by abusing Defender's update and shadow copy processes.

RedSun is a local privilege escalation vulnerability that allows an attacker to gain SYSTEM-level access. It works by abusing how Defender handles cloud-tagged files. When Defender attempts to remediate a flagged file, attackers can redirect that action to overwrite a system binary such as `C:\Windows\System32\TieringEngineService.exe`. Once overwritten, the system executes the attacker's payload with full privileges.

In addition to RedSun, a tool called UnDefend interferes with Microsoft Defender operations without requiring administrative access. In passive mode, it blocks Defender

signature updates, preventing detection of new threats. In aggressive mode, it can disrupt Defender during major platform updates, causing the service to stop responding and leaving systems unprotected.

When combined, these techniques create a clear path to weaken or disrupt Defender protections and then escalate privileges to SYSTEM, resulting in full control of the affected system. Aspire recommends immediate monitoring and defensive controls while awaiting official patches.

Aspire Protects

- Monitor for unusual Cloud Files API activity such as unauthorized sync root registrations
- Alert on creation of reparse points or directory junctions targeting system paths
- Monitor for blocked or failed Defender signature updates
- Investigate systems where Defender appears active but is not receiving updates
- Monitor for changes to `C:\Windows\System32\TieringEngineService.exe`
- Restrict execution of untrusted scripts, macros, and browser-based payloads
- Apply Attack Surface Reduction (ASR) rules to limit initial access vectors

TTPs to Watch

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker may exploit Microsoft Defender behavior to gain SYSTEM-level access (RedSun, BlueHammer)

Defense Evasion

- Impair Defenses [T1562] – The attacker may interfere with Defender functionality or block security updates to reduce detection (UnDefend)
- Modify System Image [T1601] – The attacker may overwrite legitimate system binaries with malicious payloads (RedSun)

Credential Access

- OS Credential Dumping [T1003] – The attacker may access registry hives from shadow copies to extract credentials (BlueHammer)

Persistence

- Create or Modify System Process [T1543] – The attacker may replace or create a service binary to execute code as SYSTEM (RedSun, BlueHammer)

Behavioral IoCs

- Unexpected Cloud Files provider registrations
- Use of Cloud Files API functions such as `CfRegisterSyncRoot`
- Creation of mount point reparse paths targeting `\Windows\System32`
- Modification or replacement of `TieringEngineService.exe`
- Defender signature updates failing or not applying
- Defender service appearing active but not functioning as expected

Targeted Industries

Any organization using Windows systems with Microsoft Defender enabled may be impacted.

- 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

RedSun: How Windows Defender's Remediation Became a SYSTEM File Write — nefariousplan.com

RedSun Zero-Day Shock: New Microsoft Defender Exploit Sparks Security Debate - UNDERCODE NEWS

GitHub - Nightmare-Eclipse/RedSun: The Red Sun vulnerability repository · GitHub

BlueHammer: Inside the Windows Zero-Day

GitHub - Nightmare-Eclipse/UnDefend: Repository hosting windows defender DOS tool · GitHub