UPDATE: Public Exploit Released for Unpatched Windows LegacyHive Zero-Day

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

TL;DR

A public proof-of-concept exploit called LegacyHive targets an unpatched vulnerability in the Windows User Profile Service.

An attacker with prior access to a Windows system could abuse the flaw to access and modify another user's registry hive, potentially gaining elevated code execution when an administrator logs in.

Update 7/24/2026

Microsoft has not released an official security update for the LegacyHive zero-day. However, ACROS Security has released free unofficial 0patch micropatches for supported Windows systems, including Windows 10 version 2004 and later and Windows Server 2022 and later.

The micropatch prevents the exploit from loading another user's registry hive, blocking the privilege escalation technique while organizations wait for an official Microsoft fix. The patch is deployed through the 0patch Agent and does not require a system restart.

There is still no evidence of active exploitation in the wild, and Microsoft continues to investigate the vulnerability.

Please see the free patch here.

Overview

There is an unpatched zero-day vulnerability, named LegacyHive, in the Windows User Profile Service. A CVE and CVSS score have not been assigned.

The Windows User Profile Service manages user profiles and loads user-specific registry data during logon. LegacyHive abuses the service's profile-loading process to mount another user's UsrClass.dat registry hive within the attacker's registry namespace.

Affected Products

- All currently supported Windows desktop and server installations, including systems with the July 2026 security updates installed, according to the researcher. Microsoft has not confirmed specific affected versions.

To use the public PoC, an attacker must already have access to the Windows system, credentials for a second standard user account, and the username of the account they want to target. Researchers confirmed that it works on fully patched systems. If the target is an administrator, the attacker could modify the administrator's registry settings so malicious code runs with elevated privileges when that administrator logs in or opens a specific type of file.

LegacyHive cannot be used remotely to gain initial access. An attacker would first need to compromise the system through another method, and a network firewall would not stop the exploit once that access is established. Microsoft is investigating, but no security update or formal advisory is available, and there is no evidence that the vulnerability is being exploited in attacks.

LegacyHive was released by Nightmare Eclipse, the same researcher who disclosed the RoguePlanet Microsoft Defender vulnerability that Microsoft patched in July 2026.

Aspire Protects

- Run the published Microsoft Defender for Endpoint hunting queries to check for LegacyHive activity.
  - Investigate any detected GUID folders containing `ntuser.dat` or `UsrClass.dat`, registry values pointing to `\\.\GlobalRoot` or `BaseNamedObjects`, and unexpected use of `offreg.dll`.
- Prevent administrators from logging into standard user workstations. Use dedicated administrator accounts and hardened administrative workstations.
- Disable unused local accounts and use Windows LAPS to maintain unique local administrator passwords.
- Monitor Microsoft's Security Response Center and deploy the LegacyHive security update as soon as it becomes available.

TTPs to Watch

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – An attacker may exploit LegacyHive to access and modify registry data belonging to a higher-privileged Windows user.

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

Any organization using supported Windows desktop or server systems could be affected, including:

- 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

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

GitHub - MSNightmare/LegacyHive: N/A · GitHub

LegacyHive: Video demo and analysis of Windows 0-day from NightmareEclipse