Six Zero-Days Hit Windows and Hardware in October Patch Tuesday

Microsoft's October 2025 Patch Tuesday addressed six zero-day vulnerabilities, four of which were actively exploited in the wild.

The flaws affect Windows components including the Remote Access Connection Manager (RasMan), Agere modem driver, and TPM 2.0 reference implementation, as well as AMD EPYC processors and IGEL OS.

Attackers are using several of these vulnerabilities to gain SYSTEM privileges or bypass Secure Boot protections. Immediate patching is recommended across Windows Server, Windows 10/11, and Azure environments.

Overview

October's Patch Tuesday was Microsoft's largest release of the year, with 167 vulnerabilities addressed and six zero-days confirmed. Several of these vulnerabilities affect legacy or low-level system components that operate with high privileges. They allow attackers to escalate control or compromise environments.

Actively exploited zero-days this month include:

- **CVE-2025-24990 (CVSS 7.8)** – Agere Modem Driver (Privilege Escalation)
- **CVE-2025-59230 (CVSS 7.8)** – Windows Remote Access Connection Manager (Privilege Escalation)
- **CVE-2025-47827 (CVSS 4.6)** – IGEL OS Secure Boot Bypass
- **CVE-2025-2884 (CVSS 5.3)** – TPM 2.0 Out-of-Bounds Read

Other issues include a race condition in AMD's Secure Nested Paging (CVE-2025-0033, CVSS 6.0) and an additional Agere driver vulnerability (CVE-2025-24052, CVSS 7.8).

The Zero-Day Vulnerabilities

- CVE-2025-24990 – Agere Modem Driver (EoP)
  Actively exploited vulnerability allowing attackers with local access to gain administrator privileges through untrusted pointer dereference. Exploitation does not require the modem to be in use. Microsoft has removed the vulnerable driver in the October update, permanently disabling affected hardware.

- CVE-2025-24052 – Agere Modem Driver (EoP)
  A stack-based buffer overflow in the same driver family, assessed as Exploitation More Likely. Successful attacks can grant SYSTEM-level privileges on Windows systems. The driver was also removed as part of the October patch cycle.

- CVE-2025-59230 – Windows Remote Access Connection Manager (EoP)
  Actively exploited zero-day in RasMan, used to manage VPN and dial-up connections. Improper access control enables local privilege escalation to SYSTEM. This is the first known in-the-wild exploitation of RasMan since its inclusion in Windows Vista.

- CVE-2025-2884 – TPM 2.0 Reference Implementation (Info Disclosure)
  Out-of-bounds read vulnerability in the CryptHmacSign helper function can allow exposure of sensitive memory content. While exploitation is considered less likely, this flaw weakens TPM-based cryptographic trust.

- CVE-2025-0033 – AMD Secure Nested Paging (RCE)
  A race condition during Reverse Map Table initialization could allow a malicious hypervisor to modify guest memory mappings before lock-down, impacting SEV-SNP integrity. While requiring privileged access, exploitation could compromise confidential workloads on cloud infrastructure.

- CVE-2025-47827 – IGEL OS Secure Boot Bypass
  Actively exploited vulnerability allowing attackers with physical access to bypass Secure Boot protections by loading an unverified SquashFS image. Exploitation enables persistent and kernel-level tampering.

Affected Products

- Windows 10 and Windows 11 (all supported builds)
- Windows Server 2008–2025
- Azure Confidential Computing AMD-based clusters
- IGEL OS (versions prior to 11)
- TPM 2.0 reference implementation in Windows systems
- Systems containing Agere-based modem drivers (ltmdm64.sys)

This month, attackers are shifting their focus back to what many organizations overlook, legacy code and trusted system components. Exploitation of these zero-day vulnerabilities could give attackers complete control over servers and allow persistence through Secure Boot bypasses. Even environments without outdated hardware are at risk if patching is not a priority. Aspire recommends organizations patch/update as soon as possible to avoid compromise.

Aspire Protects

- **Patch** – For all zero-days, deploy Microsoft October 2025 cumulative updates to all Windows hosts and servers. Verify update installation and successful reboots. For complete details, see the links to Microsoft's advisories below.
    - CVE-2025-24990
    - CVE-2025-24052
    - CVE-2025-59230
    - CVE-2025-0033
    - CVE-2025-2884
    - CVE-2025-47827

TTPs to Watch

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – Attackers may exploit kernel or driver flaws (Agere, RasMan) to gain SYSTEM-level privileges.
- Abuse Elevation Control Mechanism: Bypass User Account Control [T1548.002] – The attacker may bypass or abuse access control in RasMan to execute code with elevated permissions.

Persistence

- Pre-OS Boot: Bootkit. [T1542.003] – An attacker may tamper with UEFI/bootloader or the MBR to install code that runs before the OS. This grants stealthy persistence, can disable Secure Boot or endpoint defenses, and may capture keys or credentials at boot.

Defense Evasion

- Exploitation for Defense Evasion [T1211] – TPM 2.0 and AMD SEV-SNP weaknesses can be leveraged to bypass hardware-backed integrity checks.

IoCs

There are no known IoCs associated with the above vulnerability 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 October 2025 Patch Tuesday zero-days affect a wide range of Windows environments and could impact organizations across multiple sectors if exploited.

- Education
- Public Sector
- Finance
- Healthcare
- Legal
- Manufacturing
- 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-2025-2884 - Security Update Guide - Microsoft - Cert CC: CVE-2025-2884 Out-of-Bounds read vulnerability in TCG TPM2.0 reference implementation

CVE-2025-24052 - Security Update Guide - Microsoft - Windows Agere Modem Driver Elevation of Privilege Vulnerability

CVE-2025-0033 - Security Update Guide - Microsoft - AMD CVE-2025-0033: RMP Corruption During SNP Initialization

CVE-2025-47827 - Security Update Guide - Microsoft - MITRE CVE-2025-47827: Secure Boot bypass in IGEL OS before 11

CVE-2025-59230 - Security Update Guide - Microsoft - Windows Remote Access Connection Manager Elevation of Privilege Vulnerability

CVE-2025-24990 - Security Update Guide - Microsoft - Windows Agere Modem Driver Elevation of Privilege Vulnerability