ASUS Armoury Crate Vulnerability Gives Attackers Local System Access

TL;DR

A high-severity vulnerability (CVE-2025-3464) in ASUS Armoury Crate allows attackers with local access to escalate privileges to SYSTEM by abusing a flawed authorization mechanism in the AsIO3.sys driver.

No active exploitation has been observed, but users should update immediately through the Armoury Crate Update Center.

Overview

ASUS Armoury Crate, a widely used system utility preinstalled on many Republic of Games (ROG) and The Ultimate Force (TUF) devices, contains a high-severity local privilege escalation vulnerability.

Tracked as CVE-2025-3464 (CVSS 8.8), the flaw lies in the AsIO3.sys driver, which uses a hardcoded SHA-256 hash and PID allowlist instead of proper Windows access controls. Attackers with local access can exploit this by creating a hard link between a fake app and the trusted binary, tricking the driver into granting SYSTEM-level privileges. This opens the door to physical memory access, I/O control, and full OS compromise.

No active exploitation has been observed, but due to the software's large install base, there is significant risk. All Armoury Crate versions between 5.9.9.0 and 6.1.18.0 are affected.

Vulnerabilities in OEM control software continue to be exploited for local privilege escalation. If it loads a driver, it deserves the same scrutiny as core OS components. If your environment uses Armoury Crate, patch it before your organization becomes a victim.

Aspire Protects

- **Patch** – It is recommended that organizations patch CVE-2025-3464 as soon as possible. ASUS has issued a security advisory. To update:
  - Open Armoury Crate > Settings > Update Center > Check for Updates > Install any available patches.
  - Find the update in the Armoury Crate update center.
- Limit admin rights and monitor for suspicious privilege escalation activity.

- Watch for unusual usage of AsusCertService.exe or hard link behavior on endpoints.
- Identify and patch Armoury Crate on any managed devices.

TTPs to Watch

Privilege Escalation

- Abuse Elevation Control Mechanism [T1548.002] – The attacker bypassed ASUS driver protections using a manipulated hash and PID check.

Defense Evasion

- Masquerading [T1036.005] – Malicious code may be disguised as AsusCertService.exe to fool the kernel driver.

Persistence

- Boot or Logon Initialization Scripts [T1037.001] – SYSTEM access may be used to create persistent startup mechanisms.

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

Due to the widespread use of ASUS hardware in both consumer and business environments, this vulnerability could impact organizations across multiple sectors. The vulnerability especially impacts those with gaming, custom-built, or developer machines in their IT footprint.

- Gaming & eSports
- Education
- Healthcare
- Retail and eCommerce
- Manufacturing
- Software Development

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

TALOS-2025-2150 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence

NVD - CVE-2025-3464

ASUS Product Security Advisory | ASUS Global

Armoury Crate - Support