ASRock Industrial Coordinated Vulnerability Disclosure Policy
Version 1.0
Effective Date: February 13, 2026

Introduction

ASRock Industrial ("the Company") places a high priority on product security. We are committed to safeguarding our customers' information security and recognize the value of security researchers in identifying and mitigating vulnerabilities. This policy establishes a framework for collaboration with the security research community to ensure vulnerabilities are reported and remediated in a safe and effective manner.

Scope

This policy applies to all software, firmware, and hardware products developed and maintained by ASRock Industrial.

Out of scope:

- Denial-of-service attacks (DoS/DDoS) against Company services
- Social engineering attacks
- Physical intrusion or damage to Company offices or data centers
- Unauthorized access to user data (except for the minimum access necessary to demonstrate the existence of a vulnerability)

Safe Harbor

ASRock Industrial supports good faith security research conducted in accordance with this policy.

If security researchers fully comply with this policy while conducting research and reporting vulnerabilities, ASRock Industrial will:

- Treat such activities as **authorized conduct**
- Refrain from initiating legal action against the researcher
- Publicly confirm that the research was conducted in accordance with this policy should a third party initiate legal action against the researcher.

Vulnerability Reporting Channels

If you identify a potential security vulnerability, please report it through the following channel:

- Email: ASRI_security@asrockind.com

Encrypted communication (mandatory)

To ensure confidentiality during transmission, all reports must be encrypted using the Company's PGP public key.

- PGP Key download: https://download.asrock.com/IPC/PGP_Public/PGP_Public.pdf
- Note: If your report includes sensitive proof-of-concept (PoC) code or log files, encryption is required.

Recommended Report Content

To expedite processing, please include the following information:

1. Affected product model and version (including firmware/software versions)
2. Vulnerability type (e.g., Buffer Overflow, XSS, Injection)
3. Steps to reproduce or proof-of-concept (PoC) details
4. Assessment of potential impact

Handling Process and Response Timeline

ASRock Industrial commits to handling vulnerability reports according to the following process:

1. **Acknowledgment:** A confirmation email with a tracking number will be provided within three business days of receiving the report.
2. **Assessment and Validation:** The Product Security Incident Response Team (PSIRT) will validate the vulnerability. Additional information may be requested if necessary.
3. **Remediation and Updates:** Once confirmed, remediation will be developed based on risk severity. Progress updates will be provided periodically during the remediation process.
4. **Public Disclosure:** After the release of a fix, a Security Advisory will be published.

Disclosure Principles (Embargo Policy)

- Researchers must maintain confidentiality and refrain from public or third-party disclosure of vulnerability details until ASRock Industrial releases a patch or mitigation.
- In general, remediation and release will be completed within 90 days after vulnerability confirmation. If additional time is required due to complexity, disclosure timing will be coordinated with the researcher.

- The Company follows Coordinated Vulnerability Disclosure principles to balance public safety and the right to information.

Contact Information

For additional product security information or past advisories, please visit:
ASRock Industrial Security Center:
https://www.asrockind.com/security-center