A-SIT

Secure Information Technology Center – Austria

COORDINATED VULNERABILITY DISCLOSURE POLICY

Coordinated Vulnerability Disclosure Policy

Autor:
a-sit.at/
Tel: +43 (0) 1 503 19 63 – 0
Mail: vulnerability@a-sit.at
Datum: 23.03.2026

Abstract:
This CVD policy ("CVD Guideline") aims to establish a process through which security researchers can collaborate with A-SIT to improve the security of relevant products and services.

Content

Coordinated Vulnerability Disclosure Policy

Within the scope of this CVD-Policy is

A-SIT takes the security and the trust of users of products, systems, processes, or services certified by A-SIT very seriously. The responsible disclosure of security vulnerabilities helps us to ensure the security and protection of the users' privacy. We are committed to carefully reviewing security issues in products, systems, processes, or services which A-SIT is responsible for and to contributing to their remediation. However, if A-SIT has not developed the product or service, the main contact for vulnerabilities is always the manufacturer. For products or services certified or audited by A-SIT and where the vulnerability is within the certification scope, A-SIT sill contact the certificate holder and initiate the vulnerability management process defined in the applicable certification scheme.

Furthermore, we are committed to carefully reviewing and remedying security issues in products, systems, processes, or services that are developed by A-SIT.

Out of scope of this CVD-Policy is

All services, processes, and services hosted by third parties, as well as products offered by third parties, are excluded from the scope.

In the interest of the security of users of products, systems, processes, or services certified by A-SIT, our employees, the Internet as a whole, and your own safety as security researchers, the following types of testing are excluded from the scope:

- Findings from physical tests, such as access to office premises (e.g., open doors, open windows, "tailgating")
- Findings primarily derived from social engineering methods (e.g., phishing, vishing, smishing)
- Findings from applications, processes, products, or systems that are not listed in the section "Scope" above
- UI and UX issues as well as spelling or typographical errors
- Reports of non-exploitable vulnerabilities and/or indications that our services do not fully comply with "best practices" (e.g., missing security headers) are particularly out of scope
- Network-level denial-of-service vulnerabilities (DoS/DDoS) or similar
- Weaknesses in TLS configurations (e.g., support for "weak" cipher suites according to recognized standards etc.) are out of scope
- Volumetric vulnerabilities are out of scope (i.e. merely overloading our services with a high number of requests)
- Personal Data

1. Purpose

A-SIT is committed to maintaining a high level of information security for its systems, services, and users.

This Responsible Vulnerability Disclosure Policy (also referred to as Coordinated Vulnerability Disclosure – CVD) provides both a clear and precise framework for the responsible reporting, handling, and remediation of security vulnerabilities.

This particular CVD policy aims to:

- encourage security researchers to report vulnerabilities responsibly,
- protect users, partners, and systems from security risks,
- enable coordinated remediation before public disclosure,
- establish transparency and trust between A-SIT and the security community.

2. Scope

This policy applies to security vulnerabilities discovered in:

- public-facing websites, applications, and APIs operated by A-SIT,
- infrastructure and services directly managed by A-SIT,
- software or systems where A-SIT is responsible for security maintenance.

Out of scope are:

- systems not owned or operated by A-SIT,
- denial-of-service (DoS/DDoS) attacks,
- social engineering, phishing, or physical security testing,
- vulnerabilities requiring excessive disruption of services.

3. Rewards

A-SIT is a non-profit association (ZVR: 948166612). As a result of that it is not possible to offer paid rewards such as a bug bounty program. However, if you request this, after finalizing a CVD-process, A-SIT can consider to publish your name (or your alias, or comparable) and a reference on our website a-sit.at/.

4. Principles of Coordinated Disclosure

A-SIT follows the principles of Coordinated Vulnerability Disclosure as recommended by national and international best practices, including:

- **Good faith cooperation** between reporters and A-SIT
- **Confidential handling** of vulnerability information until remediation
- **Timely acknowledgment and response**
- **Risk-based prioritization** and remediation
- **Coordinated publication**, if applicable

5. Reporting a Vulnerability

Please provide valid contact information (e.g., email) so we can reach you if we have questions. For complex vulnerabilities, additional explanations or documentation may be needed. Reports without a way to contact the submitter may be processed only to a limited extent.

For anonymous reports, technical questions from A-SIT or the manufacturer cannot be answered, so related vulnerability reports may be only partially or not processed.

The use of AI-based tools (such as: large language models or comparable) must be explicitly disclosed at the time of submission of any vulnerability report, particularly including which such tools have been used. All reported findings must be independently and reproducibly verified by the submitter. Submissions consisting solely of unvalidated AI-generated content, or containing demonstrable inaccuracies (also called: “hallucinations”), will be rejected.

Security vulnerabilities should be reported as soon as possible using the contact information provided below.

Contact details

Email: vulnerability@A-SIT.at

Encryption: PGP key is retrievable via `security.txt`

Policy reference: https://a-sit.at/contact

A-SIT provides a `security.txt` file in accordance with RFC 9116 to enable automated discovery of security contact information in terms of responsible vulnerability disclosure.

6. Requirements for Vulnerability Reports

To support efficient analysis and remediation, reports should include:

- a clear description of the vulnerability,
- affected systems, processes, or services, URL, or component,
- necessary steps to reproduce the issue,
- proof of concept (PoC), if available and non-destructive,
- assessment of potential impact,
- contact details of the reporter (optional but recommended).

7. Expected Behavior of Security Researchers

A-SIT welcomes responsible security research conducted in good faith.

Researchers are expected to:

- avoid privacy violations, data destruction, or service disruption,
- limit testing to the defined scope,
- refrain from exploiting vulnerabilities beyond proof of existence,
- not publicly disclose vulnerabilities without prior coordination,
- comply with applicable laws and regulations,
- vulnerability reports based on automated tools or scans without documentation are not valid,
- exploitation tools must not be offered if they can be used by others to commit crimes,
- no tampering, compromise, or alteration of others' systems or data is allowed,
- the report must contain previously unknown vulnerabilities. Fixed issues may be reviewed but are not eligible for further processing in the CVD program.

If these conditions are met, A-SIT will not pursue legal action against the reporting party.

8. Handling and Response Process

Upon receiving a vulnerability report, A-SIT will:

(1) acknowledge receipt within a reasonable timeframe (typically within ca. 72 hours),
(2) assess and validate the reported issue,
(3) assign severity and remediation priority,
(4) work on mitigation or resolution,
(5) keep the reporter informed about progress where appropriate.

Remediation timelines depend on severity, complexity, and operational impact.

9. Disclosure and Publication

Public disclosure of vulnerabilities should only occur after:

- the vulnerability has been resolved or sufficiently mitigated, or
- a coordinated disclosure timeline has been agreed upon.

A-SIT supports coordinated publication and may acknowledge the contribution of reporters (e.g., via a "Hall of Fame"), subject to consent. The acknowledgment is only done on particular request and based on an assessment by A-SIT of the reliability and quality of the report.

10. Legal Considerations

This policy does not grant permission for activities that are illegal or outside of the defined scope.

A-SIT expects all participants to act responsibly and in accordance with applicable laws.

Reports submitted in good faith and in compliance with this policy will not result in legal action by A-SIT. That means that if you comply with this policy and act in good faith, A-SIT considers your security research to be lawful and authorized. A-SIT will thus not bring civil claims nor initiate criminal proceedings against you for violations arising solely from your research activities under this policy.

11. Data Protection

Personal data provided during the reporting process will be processed solely for vulnerability handling purposes and in accordance with applicable data protection regulations (e.g., GDPR). Besides, in any case please consider the Privacy Policy of A-SIT which is published on our website.

12. Policy Maintenance

This policy is reviewed regularly and may be updated to reflect changes in legal, technical, or organizational requirements by A-SIT.