A-SIT

Secure Information Technology Center – Austria

COORDINATED VULNERABILITY DISCLOSURE POLICY

Coordinated Vulnerability Disclosure Policy

Author:
vulnerability@a-sit.at
Tel: +43 (0) 1 503 19 63 – 0
Mail: vulnerability@a-sit.at
Datum: 01.09.2026

Abstract:
This CVD policy (or "CVD Guideline") aims to establish a process through which security researchers can collaborate with A-SIT to improve the security of relevant products, systems, processes, services, or infrastructure and to responsibly disclose vulnerabilities in a coordinated manner.

A-SIT does not provide nor offers any paid rewards nor any type of compensation such as a bug bounty program.

Content

Coordinated Vulnerability Disclosure Policy

General Introduction. A-SIT takes the security and the trust of users of products, systems, processes, services, or infrastructure very seriously. A-SIT distinguishes between (1) A-SIT assets, (2) A-SIT certified/audited assets, and (3) Third-party assets. The responsible disclosure of security vulnerabilities helps us to ensure the security and protection of the users' privacy and increase the level of security. We are committed to carefully reviewing security issues in A-SIT assets for which A-SIT is responsible for and to contributing to their remediation.

However, if A-SIT has not developed the product, system, process, service, or infrastructure (e.g., A-SIT certified/audited assets) the main contact for vulnerabilities is always the manufacturer.

1. Purpose

A-SIT is committed to maintaining a high level of information security for its A-SIT assets, A-SIT certified/audited assets 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

We are committed to carefully reviewing and remedying security issues in A-SIT assets that are owned, operated or developed by A-SIT.

The CVD policy applies to:

(1) "A-SIT assets" which are products, systems, processes, services, or infrastructure owned, operated, developed or maintained by A-SIT

(2) "A-SIT certified/audited assets" which are products, systems, processes, services, or infrastructure owned, operated, developed or maintained by a manufacturer or service provider which are either certified or audited by A-SIT. Details about A-SIT certified/audited assets are as follows:

However, A-SIT certified/audited assets are not directly in the scope of this A-SIT CVD policy. That means that where a reported vulnerability affects an A-SIT certified/audited asset within an applicable certification or audit scope, A-SIT may forward the report to the responsible manufacturer, operator, service provider or holder of a certificate (i.e., "responsible third-party") and initiate or support the vulnerability management process defined by the applicable certification or audit scheme.

If vulnerabilities in A-SIT certified/audited assets are reported, A-SIT may, where relevant in the context of a certification or audit scope, forward them "as received by A-SIT" to the responsible third-party (see above). That means that in such cases, forwarding the vulnerability report to the responsible third-party necessarily entails the disclosure of the reporter's contact details to the third-party. A-SIT does not coordinate subsequent vulnerability remediation between the reporter and the responsible third-party to which the vulnerability report is forwarded and A-SIT is not accountable for that third-party.

This policy applies to security vulnerabilities discovered in:

- Public-facing websites, applications, and APIs[1] operated by A-SIT,
- A-SIT assets which are directly managed by A-SIT,
- A-SIT assets such as software or systems where A-SIT is responsible for security maintenance.

[1] API – Application Programming Interface

The CVD policy does not apply to:

Vulnerabilities in third-party assets are outside of the scope of this A-SIT CVD. Third-party assets which are beyond the scope defined above such as products, systems, processes, services or infrastructure for which A-SIT has no responsibility for their development, operation, maintenance or security are outside the scope of this CVD policy. Those are denoted as "Third-party assets". This includes in particular:

- Products, systems, processes, services, or infrastructure either not owned nor operated by A-SIT,
- Products, systems, processes, services, or infrastructure not developed by A-SIT
- Denial-of-Service (DoS/DDoS[2]) attacks,
- Social engineering, phishing, or physical security testing,
- Vulnerabilities requiring excessive disruption of products, systems, processes, services, or infrastructure.

Submitting a vulnerability report to A-SIT does not grant authorization to test third-party assets. Security researchers must obtain the necessary authorization from the relevant developer, manufacturer, owner or operator before conducting security testing against third-party assets.

In the interest of the security of users of A_SIT assets, A-SIT certified/audited assets or third-party assets, our employees, the Internet as a whole, and your own safety as security researchers, the following types of testing are also excluded from the scope:

- Findings from A-SIT assets, or A-SIT certified/audited assets that are not listed in the section "Scope" above
- 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)
- UI[3] and UX[4] issues as well as spelling or typographical errors
- Reports of non-exploitable vulnerabilities and/or indications that our product, system, process, service, or infrastructure 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.)
- Volumetric testing, including attempts to overload A-SIT assets, or A-SIT certified/audited assets with a high volume of requests
- Privacy-related complaints or reports that do not concern a security vulnerability
- Personal data is generally out of scope. If access to personal data is absolutely necessary to demonstrate a security vulnerability, such access must be limited to the minimum necessary to demonstrate the vulnerability. Personal data must not be publicly disclosed under any circumstances.

3. No Rewards provided

A-SIT does not provide nor offers any paid rewards nor any type of compensation such as a bug bounty program.

[2] Distributed Denial-of-Service
[3] UI – User Interface
[4] UX – User Experience

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 or unverified claims (also called: "hallucinations"), will be rejected.

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

Contact details for vulnerability disclosure

The current contact details for coordinated vulnerability disclosure, including the reporting email address and information on secure communication, are published and maintained on the A-SIT website:

- a-sit.at/en/about-a-sit/contact/ (English version)
- a-sit.at/ueber-a-sit/kontakt/ (German version)

The applicable CVD policy, contact details for reporting, encryption information using a PGP[5] public key and fingerprint for secure communication, are published and maintained on A-SIT's website and through the `security.txt` mechanism in accordance with RFC[6] 9116. This includes:

- **CVD policy reference:** Permanent Link to the applicable CVD policy
- **Email:** vulnerability@a-sit.at
- **Encryption:** PGP public key for vulnerability@a-sit.at is retrievable via URL in security.txt

[5] PGP – Pretty Good Privacy
[6] RFC – Request for Comments

- **PGP fingerprint:** for the vulnerability@a-sit.at PGP public key
- **Security.txt:** Link to `security.txt` https://www.a-sit.at/.well-known/security.txt
  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 A-SIT assets or A-SIT certified/audited assets, URL[7], 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).

Vulnerability reports must contain sufficient and comprehensible technical documentation. Vulnerability reports that are solely based on the results of applying automated tools or scans and do not include any further explanatory documentation are not considered valid vulnerability reports and will not be processed as such.

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,
- report vulnerabilities that have not already been publicly disclosed. Fixed issues or vulnerabilities already known to A-SIT may nevertheless be considered and processed where appropriate.

The expected behaviours in terms of legal considerations is covered by section 10 (“Legal Considerations”) of this CVD policy.

In general, A-SIT expects that researchers act in good faith, comply with this CVD policy, remain within the defined scope, and avoid intentionally accessing, modifying, deleting, or exfiltrating data beyond what is necessary to demonstrate a vulnerability.

[7] URL – Uniform Resource Locator

8. Handling and Response Process

Upon receiving a vulnerability report, A-SIT will:

(1) acknowledge receipt within a reasonable timeframe (aims typically within ca. 3 business days),
(2) assess and validate the reported issue,
(3) assign severity applying a CVSS[8] 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.

A-SIT assumes to communicate with natural persons. If A-SIT has reasons to believe that the report is automated, like AI generated or low effort reports, A-SIT might neither acknowledge receipt nor keep the reporter informed (steps 1 and 5 above). Still the remediation process will be conducted.

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, within the defined scope and in compliance with this policy, A-SIT considers such activities to be authorized for the purposes of this policy. This authorization applies only to activities within the defined scope of this CVD policy. A-SIT will neither seek civil remedies nor initiate criminal proceedings, nor support legal action against researchers except where required by law or where there is evidence of malicious, abusive, or intentionally harmful conduct solely for activities covered by this CVD policy, provided that the researcher acts in good faith, remains within the defined scope and complies with this policy.

If you act in good faith, comply with this policy, remain within the defined scope, and avoid intentionally accessing, modifying, deleting or exfiltrating data, A-SIT will not initiate or support legal action against you in relation to activities covered by this policy, except where required by law or where there is evidence of malicious or abusive conduct.

[8] CVSS – Common Vulnerability Scoring System

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.