IT-Sicherheit | ETH Responsible Disclosure Policy

Introduction

Responsible disclosure is a process that allows IT-security researchers to safely report found vulnerabilities to the responsible personnel within your organization. This document describes the content of the policy.

ETH Zurich strives to implement IT-security best practices to protect data and systems. This policy is intended to give security researchers guidelines for conducting vulnerability discovery activities and to convey our preferences on how to submit discovered vulnerabilities to us. Further, we describe what systems and types of research are covered under this policy.

Guidelines

Under this policy, “research” means activities in which you:

- notify us as soon as possible after you discover a substantially real or potential IT-security issue.
- make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- only use exploits to the extent necessary to confirm a vulnerability’s presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.
- provide us a reasonable amount of time to resolve the issue before you disclose it publicly.
- do not submit low-quality reports.

If a vulnerability affecting any ETH Zurich systems is submitted in compliance with the specified rules and the reporter acts in good faith, without fraudulent intent nor intention to do harm, the ETH Zurich will not pursue civil or criminal action against you.

Test methods

The following test methods are explicitly forbidden:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data.
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing.

Once you’ve established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), you must stop your test, notify us immediately, and not disclose this data to anyone else.

Scope

This policy applies to the following systems and services of the domains associated with:

- ethz.ch (including all on-premises hosts with private IPs (e.g. RFC1918)

- As per WHOIS
  - the organization (“org” field) corresponding to the ORG-ETHZ1-RIPE entry.
  - the admin-c or tech-c roles defining "HE688-RIPE" (Hostmaster ETHZ).

Any services or systems of the domain(s) not listed above are excluded from scope and are not authorized for testing. Vulnerabilities found in systems of other institutions within the ETH Domain (e.g. Empa, Eawag, etc.) fall outside the scope of this policy and should be reported directly to the annex according to their disclosure policy (if any). If you aren’t sure whether a system is in scope or not, contact the responsible security team for the system’s domain name listed in a WHOIS registry, e.g. https://www.ripe.net).

Reporting a vulnerability

Contact and submission

Complete the form below including details of your discovery. If available, please include your PGP public key so that the ETH Zurich can validate submissions.

Submit vulnerability findings only to ***security@ethz.ch***

For encrypted communication, use the PGP key of ***security@ethz.ch***

- Key ID: 0x6EEEFBFFD6437004
- Fingerprint: 2CC2 9A19 4B25 DDD0 B750 B48B 6EEE FBFF D643 7004

Provide enough information as possible to enable the vulnerability to be reproduced. This helps to speed up the process. For more complex vulnerabilities, the ETH Zurich might need to communicate directly with you. Please provide at least an email address or phone number.

What we would like to see from you

In order to help us triage and prioritize submissions, we recommend that your reports:

- describe the location the vulnerability was discovered and the potential impact of exploitation. Submissions which do not include this information will be ignored.
- offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- provide references relevant to the vulnerability: e.g., CVE, security bulletins, etc.

You can choose to send your vulnerability reports anonymously to ETH Zurich. Submissions should be in English or German, if possible.

What you can expect from us

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible. ETH Zurich will

- decide on a case-by-case basis if a response is necessary and warranted.
- treat reports as confidential and will not share the personal data of the reporting parties or receiving organisation without their respective consent.

- bring the vulnerability to the attention of the responsible parties, depending on the entities concerned and the nature of the vulnerability established. The owner of the affected IT system remains responsible for the system and potential remediation activities.

Acknowledgement & Bounties

ETH Zurich is not in the position to acknowledge submissions through the publication of research findings (e.g. accreditation or *Hall of Fame* listings) or through payment of bug bounty rewards. We hope that researchers will submit findings based on good faith and in the interest of promoting IT-security on a global scale.

Vulnerability Submission Form

Report your submission to: ***security@ethz.ch***

Share where you found the vulnerability.
Examples include hostname, URL, IP address or service.

Describe the vulnerability and its potential impact.

Give a detailed description of the steps needed to reproduce the vulnerability.
*Links to proof of concept scripts or screenshots are helpful**

Is there anything else we should know?

You may share your contact information so that we can get in touch with you, if needed.
Email address, telephone number, other sites

Include your PGP signature to help prove your identity.

* Note that attachments, such as scripts, programs, screenshots, etc. may be stripped out by virus scanning programs or may cause an entire email to be blocked completely. Please consider the content of the information being sent.