Responsible Vulnerability Disclosure Policy

Indian Institute of Science

Objective

Indian Institute of Science is committed to ensuring the confidentiality, integrity and availability of its' information systems. This Responsible Vulnerability Disclosure Policy aims to enhance the security of the Institute's systems, networks, and digital information assets by establishing a process for reporting vulnerabilities. We encourage security researchers and ethical hackers who have identified potential vulnerabilities in the Institute's Information Technology systems to use these directions to report them responsibly and promptly to our security team.

Scope

The following will be in scope of this Responsible Vulnerability Disclosure Policy.

1. *.iisc.ac.in domain and subdomains
2. Public facing APIs
3. Institute's mobile applications

The following will be out of scope of this Policy.

1. Third-party services / applications
2. Personal devices of students/staff
3. Physical security of systems
4. Social engineering attempts
5. Denial of Service (DoS) attacks
6. Vulnerabilities identified through automated tools

Disclosure process

1. Submit the report via email to ciso@iisc.ac.in with the subject line "Responsible Vulnerability Disclosure Report."
2. The report should include:
    a. Detailed description of the vulnerability
    b. Steps to reproduce
    c. Proof of concept (if available)

    d. Potential impact assessment
    e. Suggested remediation steps
    f. Contact details of the reporter
3. Any testing should be limited to non-intrusive methods and must not compromise the security or privacy of any user or system. Avoid actions that could lead to disruption, unauthorized access or destruction of data. If a vulnerability is identified that leads to system access, do not proceed further and ensure immediate reporting.
4. Do not disclose - either publicly or to other parties - vulnerabilities or associated information without prior consent from the institute. Responsible disclosure requires providing the institute sufficient time to investigate, mitigate, and respond to any reported vulnerability.
5. IISc reserves its right to validate the reported issues as a "vulnerability" or "not a vulnerability".
6. IISc does not support any violation of applicable laws and / or regulations. Hence care should be taken that the activities undertaken during the identification of a vulnerability does not result in a breach of these.

Our commitment

The Institute hereby commits to

1. Not pursue legal action for good faith research that is in compliance to this Policy.
2. Maintain confidentiality of reports.
3. Acknowledge receipt within five working days of receiving the report.
4. Keep researchers informed of progress.
5. Fix validated vulnerabilities promptly.
6. Notify the researcher once the issue is fixed.
7. Provide due credit (with permission of the researchers).

The Institute values the contributions of ethical security researchers. While we do not currently offer monetary rewards, we recognise the efforts of those who follow responsible disclosure practices and may, upon request and at our discretion, offer public acknowledgment for valid reports on our website.