ITSecuConsult

IT SECURITY CONSULTING

Responsible Disclosure Policy

V1.0 - Last Updated: 16-12-2025

Introduction

At ITSecuConsult, we value the security and privacy of our systems and users. We believe that working with the security community is essential for keeping our services safe. If you believe you have discovered a security vulnerability in any of our systems or services, we encourage you to report it to us in accordance with this policy.

By adhering to these guidelines, you help us resolve issues quickly and protect our community, and we, in turn, commit to working with you openly and responsibly.

Reporting a Vulnerability

Please send your vulnerability report immediately via email to: **security@itsecuconsult.com**

What to include in your report

- **Sufficient Detail:** Provide enough information to reproduce the vulnerability, including:
  - The website, domain, IP, or service where the vulnerability was observed.
  - A brief description of the type of vulnerability (e.g., XSS, SQL Injection, broken access control).
  - Detailed steps or a benign, non-destructive Proof of Concept (PoC) to reproduce the issue. Screenshots or scripts are helpful.
- **Impact:** Describe the potential impact of the vulnerability if exploited.
- **Contact Information (Optional):** You may submit anonymously, but if you wish to receive updates or credit, please provide your contact information.

Our Guidelines for Researchers

When conducting security research on ITSecuConsult systems, we require that you:

1. **Do Not Exploit:** Do not take advantage of the vulnerability beyond what is necessary to confirm its existence. This includes:
   - Downloading, deleting, or modifying any data other than your own.
   - Exfiltrating data or establishing persistent command line access.
   - Compromising or violating the privacy of our users or staff.
2. **Minimize Disruption:** Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.

3. **Stay in Scope:** Only perform testing on ReguLight's own systems and services. Do not test systems or services belonging to third-party vendors.
4. **Prohibited Activities:** The following test methods are strictly **not authorized** and considered **out of scope**:
   - Any form of Denial of Service (DoS or DDoS) attack.
   - Social engineering (e.g., phishing) or physical security attacks against ITSecuConsult staff or infrastructure.
   - Using high-intensity, automated, or destructive scanning tools.
   - Submitting reports detailing non-exploitable vulnerabilities or best-practice deficiencies (e.g., missing security headers, weak TLS configuration) unless a direct, chained attack can be demonstrated.
5. **Confidentiality:** Do not disclose the vulnerability publicly or to any third party until we have resolved the issue and authorized public disclosure.

Our Commitment to You

If you make a good faith effort to comply with this Responsible Disclosure Policy during your security research, we commit to the following:

- **Safe Harbor:** We will not recommend or pursue legal action against you for research conducted in accordance with this policy.

- **Communication:** We will acknowledge receipt of your report within **5 business days** and keep you informed of our progress toward resolving the vulnerability.

- **Remediation:** We will strive to resolve the issue as quickly as possible. The timeline will depend on the complexity and severity of the vulnerability.

Thank you!