Vulnerability Disclosure Policy

1 May 2024

Welcome to Peak3's Security Vulnerability Disclosure Policy. We take cyber security issues very seriously and recognise the importance of privacy and security in our websites, products and services. As such, we are committed to addressing and reporting security issues through a coordinated and constructive approach; and appreciate your efforts in helping us maintain the security of our websites, products and services.

Please read this policy carefully before reporting any vulnerabilities to ensure compliance.

Scope:

This policy pertains exclusively to vulnerabilities in Peak3's websites, products and services, subject to the following conditions:

- In-scope vulnerabilities must be original, previously unreported, and not discovered through internal procedures.
- Volumetric vulnerabilities, including overwhelming a service with a high volume of requests, are not within scope.
- Non-exploitable vulnerabilities or deviations from "best practice," such as missing security headers, are not considered in scope.
- TLS configuration weaknesses, like "weak" cipher suite support or TLS1.0 presence, are excluded from scope.
- Applicable to all parties, including Peak3 staff, third-party suppliers, customers, and users.

Reporting a Vulnerability:

To report an in-scope security vulnerability, please contact us via support@peak3.com. In your submission, include:

- The specific website, page, firmware, or software product where the vulnerability is observed.
- A brief description of the vulnerability type (e.g., XSS vulnerability).
- Provide a benign, non-destructive proof of exploitation whenever possible to expedite triage and reduce duplicate reports or malicious exploitation.
- Indicate your preferred method of communication for further information or updates on vulnerability resolution.

What to Expect:

Upon submission, you will receive an acknowledgment within 72 working hours. Our team will triage the report promptly and notify you if further information is required or if the vulnerability is deemed out of scope or a duplicate.

Bug fix priority is determined by impact severity and exploit complexity. While reports may take time to triage or address, you can inquire about the process status every 14 days to allow our teams to focus on resolutions.

Guidance for Security Researchers:

- Please do not exfiltrate data. Instead use a proof of concept to demonstrate a vulnerability.
- Refrain from using invasive or destructive security scanning tools.
- Protect the privacy of Peak3's customers, users, staff, and systems.
- Communicate vulnerabilities only through approved channels specified in this policy.
- Do not modify Peak3 data or disrupt services.
- Avoid social engineering, phishing, or physical attacks on Peak3 staff or infrastructure.

- Do not disclose vulnerabilities to third parties or the public before Peak3 confirms mitigation.

Data Handling:

Please securely delete any retrieved data when no longer necessary or within one month of vulnerability resolution.

Legal Compliance:

This policy aligns with common vulnerability disclosure practices and does not authorize actions contrary to the law or Peak3's legal obligations.

Thank you for contributing to the security of Peak3. We value your partnership in maintaining a safe environment for our users and systems.