Kraftful Vulnerability Disclosure Policy

Introduction

At Kraftful, we take the security of our systems and the protection of our users' data very seriously. We value the contributions of the security research community in helping us identify and address vulnerabilities. This Vulnerability Disclosure Policy outlines the guidelines for conducting security research on our systems and how to report any discovered vulnerabilities to us.

Authorization

We authorize good-faith security research conducted in accordance with this policy. If you follow these guidelines, we will not pursue legal action against you for your research activities. If a third party initiates legal action against you for research conducted in compliance with this policy, we will make our authorization known.

Guidelines

When conducting security research under this policy, please:

- Notify us as soon as possible after discovering a potential security issue.
- Avoid violating privacy, disrupting user experience, damaging production systems, or manipulating data.
- Use exploits only to the extent necessary to confirm a vulnerability. Do not use exploits to compromise or exfiltrate data, establish command line access, or pivot to other systems.
- Give us a reasonable amount of time to address the issue before publicly disclosing it.
- Refrain from submitting a high volume of low-quality reports.
- Stop testing and notify us immediately if you encounter any sensitive data (e.g., personally identifiable information, financial information, proprietary information).

Test Methods Not Authorized

The following test methods are not authorized under this policy:

- Network denial of service (DoS or DDoS) tests or tests that impair access to or damage systems or data.
- Physical testing (e.g., office access, tailgating), social engineering (e.g., phishing, vishing), or non-technical vulnerability testing.
- Full red-team penetration testing involving unauthorized access to our servers.

Scope

This policy applies to the following systems and services:

- `*.kraftful.com`

Any services not explicitly listed above are excluded from the scope and are not authorized for testing. If you are unsure whether a system is in scope, please contact us at `security@kraftful.com` before starting your research.

Reporting a Vulnerability

To report a vulnerability, please email us at `security@kraftful.com` with the following information:

- The location of the discovered vulnerability and its potential impact.
- A detailed description of the steps to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- Your report should be in English, if possible.

You may submit reports anonymously. If you provide contact information, we will acknowledge receipt of your report within 3 business days.

What You Can Expect From Us

When you share your contact information with us, we commit to:

- Acknowledging receipt of your report within 3 business days.
- Confirming the existence of the vulnerability and being transparent about our remediation process.
- Keeping you informed about the progress of resolving the issue.

Please note that Kraftful does not provide monetary rewards for vulnerability reports. By submitting a vulnerability, you waive any claims to compensation.

Questions

If you have any questions about this policy or suggestions for improvement, please contact us at `security@kraftful.com`.

Thank you for helping us keep Kraftful secure!

History

Date	Changes	Version
04/17/2023	Initial version	1.0