Vulnerability Disclosure Policy
Zenaciti Corporation

Introduction

Zenaciti Corporation ("Zenaciti") is committed to security and privacy. This policy is intended to give security researchers guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

This policy describes what systems and types of research are covered under this policy, how to send us vulnerability reports, and how long we expect security researchers to wait before publicly disclosing vulnerabilities.

We take security seriously - we are a security firm. If you report something, we will review it and react in a reasonable and timely manner.

This policy covers all assets of Zenaciti Corporation including zenaciti.com, andrewplato.com, foundersusermanual.com, toniplato.com, and zenaciti.site.

Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized we will work with you to understand and resolve the issue quickly. Zenaciti will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.

Guidelines

Under this policy, "research" means activities in which you:

- Notify us as soon as possible after you discover a real or potential 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 Zenaciti a reasonable amount of time to resolve the issue before you disclose it publicly.
- Do not submit a high volume of low-quality reports.

Once you have 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.

Test methods

The following test methods are not authorized:

- 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
- War-dialing or similar brute force attacks against communication systems

Scope

This policy applies to hosts and systems for the following domains:

- Zenaciti.com
- Zenaciti.site
- Andrewplato.com
- Foundersusermanual.com
- Toniplato.com
- Floofy.house

Zenaciti hosts most services at third party vendors, such as Cloudflare, AWS, and such. Those third party hosted locations are specifically excluded from the scope of this policy. Vulnerabilities found in systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any).

Zenaciti does not publish a list of systems we own directly. Therefore, contact us at admin@zenaciti.com to validate if a system you are testing is in scope for this policy.

Reporting a vulnerability

We accept vulnerability at admin@zenaciti.com. Reports may be submitted anonymously. If you share contact information, we will acknowledge receipt of your report within 10 business days.

Zenaciti does not have a "bug bounty" program. However, we may provide a gratuity payment for your diligence and efforts.

A GPG Key to encrypt messages is located at https://zenaciti.com/.well-known/admin-zenaciti_public.asc .

What we expect from you:

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

- List the specific host, name, IP address, etc.
- Describe the location the vulnerability was discovered and the potential impact of exploitation.

- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- Be in English.

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.

- Within 10 business days, we will acknowledge that your report has been received.
- To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues.
- We will give you credit for the discovery, if it is legitimate.

Questions

Questions regarding this policy may be sent to admin@zenaciti.com. We also invite you to contact us with suggestions for improving this policy.