DEFEND

Version 1.0 | 28th March 2024

Vulnerability Disclosure Policy

DEFEND is committed to ensuring the security of its systems and website by protecting information. This policy is intended to give security researchers clear 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.

We encourage you to contact us to report potential vulnerabilities in our systems.

Authorisation

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorised. We will work with you to understand and resolve the issue quickly and DEFEND 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 authorisation 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 us 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've 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 authorised:

- Network 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

Version 1.0 | 28th March 2024

Vulnerbility Disclosure Policy

Scope

This policy applies to all websites and domains that DEFEND NZ Limited own and operate.

Any service not expressly stated above, such as any connected services, are excluded from scope and are not authorised for testing.

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).

Though we develop and maintain other internet-accessible systems or services, we ask that active research and testing only be conducted on the systems and services covered by the scope of this document. If there is a particular system not in scope that you think merits testing, please contact us to discuss it first. We will increase the scope of this policy over time.

Reporting a vulnerability

Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all users of a product or service and not solely DEFEND, we may share your report with the relevant party, where it will be handled under their coordinated vulnerability disclosure process. We will not share your name or contact information without express permission.

We accept vulnerability reports via disclosure@defend.co.nz Reports may be submitted anonymously. If you share contact information, we will acknowledge receipt of your report within 5 business days.

We do not support PGP-encrypted emails. For particularly sensitive information, we may respond with an appropriate mechanism for secure transmission.

What we would like to see from you

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

- 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 5 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.

Questions

Questions regarding this policy may be sent to disclosure@defend.co.nz
We also invite you to contact us with suggestions for improving this policy.