Responsible Disclosure Policy

Introduction

Mando ("We", "Us", "Our") appreciates and values the identification and reporting of security vulnerabilities carried out by well-intentioned, ethical security researchers ("You").

This vulnerability disclosure policy applies to any vulnerabilities you are considering reporting to us. We recommend reading this vulnerability disclosure policy fully before you report a vulnerability and always acting in compliance with it.

We do not offer a bug bounty program or monetary rewards for responsible disclosures and compensation requests will not be considered in compliance with this Responsible Disclosure Policy.

Reporting

If you believe you have found a security vulnerability, please submit your report to us using the following email address: info@mando.co.uk

Your report should include details of:

- The website, domain, IP or page where the vulnerability can be observed.
- Steps to reproduce which should be a benign, non-destructive, proof of concept. This helps to ensure that the report can be triaged quickly and accurately.

If you have any concerns or queries with regard reporting, please email info@mando.co.uk for advice.

What to expect

We aim to confirm receipt of your vulnerability report within 5 working days and triage your report within 10 working days. We also aim to keep you informed of our progress and completion of any remediation activities. We may contact you if we require further information regarding your report.

Remediation of any reported vulnerabilities are assessed based upon their impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status but we ask that you avoid doing so more than once every 14 days to allow our teams to focus on the remediation.

Guidance

You must NOT:

- Break any applicable law or regulations.
- Access unnecessary, excessive or significant amounts of data or modify data in our systems or services.
- Disrupt our services or systems, use high-intensity invasive or destructive scanning tools to find vulnerabilities or attempt any form of denial of service.
- Submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with "best practice", for example missing security headers.

- Submit reports detailing TLS configuration weaknesses, for example “weak” cipher suite support or the presence of TLS1.0 support.
- Social engineer, ‘phish’ or physically attack our staff or infrastructure.
- Demand financial compensation in order to disclose any vulnerabilities.

You must:

- Always comply with data protection rules and must not violate the privacy of our users, staff, contractors, services or systems. You must not, for example, share, redistribute or fail to properly secure data retrieved from the systems or services.
- Securely delete all data retrieved during your research as soon as it is no longer required or within 1 month of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).

Legalities

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause us to be in breach of any legal obligations.