Vulnerability Disclosure Program - orthodox.ai

Effective: Monday, November 4th, 2019.

Maintaining the security of our products is a high priority at orthodox.ai. Our products provide valuable services and contain access to our customers' proprietary assets and information.

The security researcher community regularly makes valuable contributions to the security of organizations and the broader Internet, and orthodox.ai recognizes that fostering a close relationship with the community will help improve our own security. So if you have information about a vulnerability in our website or web application, we want to hear from you!

Scope

Any properties owned by orthodox.ai (*.orthodox.ai) are in scope for the program.

Customers of orthodox.ai are out of scope.

Safe Harbor

orthodox.ai, Inc. pledges not to initiate legal action against researchers for penetrating or attempting to penetrate our systems as long as they adhere to this policy.

Submitting a Vulnerability

To submit a vulnerability report to orthodox.ai's Security Team, please email your full report to: security@orthodox.ai

What we would like to see from you:

- Well-written reports in English will have a higher chance of being accepted.
- Reports that include proof of concept code will be more likely to be accepted.
- Reports that include only crash dumps or other automated tool output will most likely not be accepted.
- Reports that include products not in scope will most likely be ignored.
- Include how you found the bug, the impact, and any potential remediation.
- Any plans for public disclosure.

What you can expect from us:

- A timely response to your email (within 2 business days).
- An open dialog to discuss issues.
- Notification when the vulnerability analysis has completed each stage of our review.
- An expected timeline for patches and fixes (usually within 120 days).
- Credit after the vulnerability has been validated and fixed.

Public Notification

If applicable, orthodox.ai will coordinate public notification of a validated vulnerability with you. When possible, we would prefer that our respective public disclosures be posted simultaneously.

In order to protect our customers, orthodox.ai requests that you not post or share any information about a potential vulnerability in any public setting until we have researched, responded to, and addressed the reported vulnerability and informed customers if needed.