muddy boots

driven by TELUS

Disclosure Policy

April 2018

Muddy Boots Disclosure Policy

As a software development company, keeping our customer data safe is a primary concern. If you are a customer or security researcher and have discovered a security vulnerability in one of our products, we would appreciate your help by disclosing it to us in a responsible manner and allowing us to fix it before any public disclosure.

Muddy Boots will cooperate with customers and researchers who report vulnerabilities to us in accordance with this policy. We will verify issues and fix vulnerabilities to ensure the best possible security of our products. We won't take legal action against, suspend, or terminate access to services for those who discover and report security vulnerabilities responsibly. Muddy Boots reserves all of its legal rights in the event of non-compliance with this policy.

By contacting us you may provide us with an email address, name and other personal information. This information will be processed in accordance with our GDPR policy and our Privacy Policy - https://en.muddyboots.com/policies

Reporting

You can share the details of any suspected vulnerabilities directly with the Muddy Boots Security Team by emailing us at security@muddyboots.com.

We ask that you do not publicly disclose these details outside of this process without explicit permission. We request that you include the following information to help us to triage and respond to issues quickly.

- Vulnerable URL - the endpoint where the vulnerability occurs
- Vulnerability type - the type of the vulnerability (SQLi, XSS, CSRF)
- Steps to reproduce - step-by-step information on how to reproduce the issue
- Proof of concept - a demonstration of the attack - screenshots or video
- Attack scenario - an optional example attack scenario may help demonstrate the risk and get your issue resolved faster.

If you are unable to provide this level of detail but feel you have discovered a security issue, please contact us anyway and we will work with you to assess it.

Scope

Muddy Boots Software Ltd products and public websites are considered in scope for this policy. Any third party service integrated or linked to any product or website is explicitly out of scope.

Exclusions

- Attempting any type of Denial of Service attack
- Use of automated vulnerability scanners
- Social Engineering of staff or customers
- Cookie flags
- Login/Logout CSRF
- Missing additional security controls, such as HSTS or CSP headers
- Mobile issues that require a Rooted or Jailbroken device

Muddy Boots Disclosure Policy

- Reset link expiration or password complexity
- SPF, DKIM, DMARC issues
- Self-XSS or other behaviour where you can only attack yourself.

Please do not deliberately attempt to access, modify, or destroy data that does not belong to you. If this does happen we request that you contact us urgently at security@muddyboots. com so that we can work quickly to resolve the issue.

Our commitment to you

If you identify a security vulnerability in compliance with this policy, Muddy Boots commits to:

- Your vulnerability report will be read and assessed by a security analyst
- Acknowledge receipt of your vulnerability report in a timely manner, typically within 3 working days
- Work with you if necessary and to notify you when the vulnerability is fixed
- Publicly thank you for your responsible disclosure and helping us keep our customers safe.

This policy is reviewed regularly by Muddy Boots Software Ltd. Last updated November 2020.

CONTACT US
t. +44 (0)1989 780540
e. security@muddyboots.com
w. www.muddyboots.com
@MuddyBootsLtd