Tribepad

Responsible Vulnerability Disclosure Program

Publication date: 20/01/2021
Last updated: 27/06/2022

1.0 Vulnerability disclosure program **2**
1.1 Service level agreement 2
1.2 Terms and conditions 3
1.3 Report style 3
1.4 Disclosure scope 3
1.5 Exclusions 4
1.6 Reward criteria and definitions 5
1.6.1 Critical 5
1.6.2 High 5
1.6.3 Medium 5
1.6.4 Low 5

1.0 Vulnerability disclosure program

We believe that security comes first and that white hat hackers play a vital role in strengthening the world's security posture.

If you believe that you have discovered a vulnerability then please disclose this to us by emailing security@tribepad.com. We will work with you to validate your submission and remediate the vulnerability as soon as possible.

Before you submit any vulnerabilities please review **all** the sections in this document.

1.1 Service level agreement

Please allow up to 2 business days for someone from the security team to respond to your disclosure request.

Please allow up to 4 weeks for the processing of payments for bounty rewards. Rewards are paid either via PayPal or bank transfer and require an invoice being sent to us detailing

- Your full name and email address
- The reward amount (agreed with Tribepad)
- The company you are requesting money from (Tribepad)
- Reason for payment (bug bounty reward)
- The bank account to be paid, including
    - Bank name
    - Bank address
- Date and time

1.2 Terms and conditions

Any vulnerabilities that are discovered by participants are to be i) reported via the specified communication channel to Tribepad and ii) **must not** be reported directly to any of Tribepads clients.

All participants of the program:

Must

- Respect the sensitivity of any discovered vulnerabilities
- Respect the privacy of Tribepad
- Disclose vulnerabilities **only** to security@tribepad.com
- Retest any discovered vulnerabilities when prompted (for eligibility of reward)

Must not

- Report discovered vulnerabilities to Tribepad clients
- Attempt to access any accounts or private data that does not belong to you
- Attempt to modify or destroy any data of accounts that do not belong to you

Failure to adhere to any of the above will result in no bounty reward and possible legal action being taken, depending on the nature, severity and the sensitivity of the situation.

1.3 Report style

When reporting discovered vulnerabilities to us, please ensure that the following details are included

- Issue title
- Vulnerability type
- How does it impact the system and/or user(s)?
    - Impact level (severity)
    - Impact description
- What can be done to mitigate and/or remediate the issue?
    - Techniques to apply to code (where applicable)
    - Techniques to apply to infrastructure (where applicable)
    - Explain / expand where possible.
- Please provide a proof of concept

Failure to include relevant details will result in lack of reward.

1.4 Disclosure scope

The following URLs are in scope for the program. **Do not test** outside of these domains / URLs, as vulnerabilities on these **will not** be eligible for reward.

- https://windmill.tribepad.com/
- https://support.tribepad.com
- https://tribepad.com
- https://manage.tribepad.com
- https://insights.tribepad.com

Accepted vulnerabilities include:

- Enumeration (only eligible for reward if information is Confidential)
- Stored XSS
- Reflected XSS
- SQL injection
- CSRF
- Open redirection
- RCE
- Token Vulnerability
- Unrestricted file upload
- SSRF
- Privilege escalation
- IDOR
- DoS (limit requests to produce proof of concept)
- Web cache poisoning
- CORS
- Broken access control

NOTE: Vulnerabilities are only considered valid when participants provide a proof of concept for the exploit. If participants are unable to prove that the vulnerability can be exploited, then bounty rewards will not be eligible.

1.5 Exclusions

The following types of attacks / vulnerabilities are **excluded** from the scheme. Please refrain from the following:

- Social engineering
- Component vulnerabilities (out of date libraries)
- Brute force attacks
- MITM attacks
- Distributed Denial of Service
- Spamming
- Physical attempts against Tribepad and data centres

Rewards will be not be **eligible** under the following circumstances:

- Discovered vulnerabilities are already known by Tribepad (these will be classed as duplicates)
- Discovered vulnerabilities are disclosed to Tribepad clients
- Discovered vulnerabilities are against a product and/or feature that is either i) being decommissioned or ii) is currently unused

Excluded platform features include:

- Groups
- Communities
- Clusters
- Connections
- Messages

These areas of the platform **will not** be eligible for rewards.

1.6 Reward criteria and definitions

Please find our definitions of each severity / impact level below. This is what we will be accepting for the level rewards.

Severity / Impact	**Amount (in GBP)**
Critical	£300
High	£175 - £250
Medium	£75 - £150
Low	£25 - £50
Accepted risk or informational **(unless the information is critical such as a password)**	No reward.

1.6.1 Critical

- Tribepad servers, databases or personal data records can be compromised via the web application which results in privilege escalation, data extraction, data damage or account takeover.
- Informational or enumeration counts here if the information is a database, server or administrator user password.

1.6.2 High

- The vulnerability exploit is possible on multiple accounts, resulting in privilege escalation, data damage, data leak or account takeover of other user accounts.
- User impact:

    - Affects multiple candidate accounts that do not belong to the participant.
    - Affects multiple recruiter accounts through privilege escalation.
    - Privilege escalation must originate from the candidate account.

1.6.3 Medium

- The vulnerability exploit is possible on multiple accounts, only resulting in data damage or defacement.
- User impact:
    - Affects multiple candidate accounts that do not belong to the participant.
    - Affects multiple recruiter accounts that do not belong to the participant.

1.6.4 Low

- The vulnerability exploit is possible on the account in use and does not lead to other accounts.
- User impact:
    - Affects a single candidate account that belongs to the participant.
    - Affects a single recruiter account that belongs to the participant.

The table below shows the vulnerabilities and payouts that fit within these brackets.

Accepted Vulnerabilities	**Payout £**			
	Low	**Medium**	**High**	**Critical**
Enumeration (if information is confidential)	This is decided once the report is reviewed.			
Stored XSS	50	100	200	300
Reflected XSS	50	100	200	300
Broken access control	50	100	200	300
SQL injection	50	150	250	300
CSRF	25	75	175	
Open redirect	25	75	175	300
RCE			250	300
Token Vulnerability	25	75	175	300
Unrestricted file upload	50	100	200	300
SSRF	50	150	250	300
Privilege escalation			250	300
IDOR	50	100	200	300