Vulnerability Disclosure Policy

This vulnerability disclosure policy applies to any vulnerabilities you are considering reporting to us. Please read this policy before submitting a report and always act in compliance with it.

We highly value the efforts of security researchers who help us keep our systems safe. As a token of our appreciation, we may, at our sole discretion, offer monetary rewards for responsible disclosure of security vulnerabilities that are new, significant, and within scope.

We will not pay a reward (and we will be really upset) if we detect:

- Social engineering directed at the company's employees
- Attempt to access arbitrary user's account or data or another vulnerability post- exploitation not required to demonstrate the bug presence
- Distributed network/request flooding and other resource exhaustion attacks. Automated scanning tools must be limited to 5 request per second (300 requests per minute) to one target host summing up all tools and threads running in parallel and must not exceed 5 parallel requests at the same time (5 threads).

Please use your own accounts, phone numbers, etc to conduct your research. Do not try to gain access to others' accounts or any confidential information.

We do not initiate security investigations regarding:

- Messages from security scanners and other automated systems without clear PoC and impact;
- Vulnerability reports based on software/protocol versions not indicating the actual usage/exploitation;
- Reports about the absence of a protection mechanism or non-compliance with recommendations (for example, the absence of a CSRF token) without indicating real negative consequences;
- Self-XSS;
- Framing;
- Social engineering;
- Clickjacking;
- SPF/DKIM/DMARC issues;
- Man-in-the-Middle attacks

- Vulnerabilities in partner services and products that do not directly affect the security of the company's services.
- Infrastructure vulnerabilities, including:
    - Server configuration issues (e.g. open ports, TLS versions, etc.)
    - Issues related to SSL certificates
    - DNS configuration issues

Strictly prohibited actions:

- DoS / DDoS attacks;
- Threats/harm to company employees.

Reporting

If you believe you have discovered a security vulnerability, please submit your report to cybersecurity@1win.pro.

When submitting your report, please include:

- The website, IP address, or specific page where the vulnerability can be observed.
- A brief description of the vulnerability type (e.g., “XSS vulnerability”).
- Step-by-step instructions to reproduce the issue (preferably a non-destructive proof of concept).

Report template

Summary:

[add summary of the vulnerability]

Steps To Reproduce:

[add details for how we can reproduce the issue]

1. [add step]

1. [add step]

1. [add step]

==Provide the request in curl format, if possible==

Supporting Material/References:

[list any additional material (e.g. screenshots, logs, etc.)]

** [attachment / reference]*

Rewards

We may, at our sole discretion, provide monetary rewards for eligible vulnerability reports. The amount of the reward will depend on the severity, impact, and quality of the report, as well as other factors deemed relevant by our security team. Not all reports will qualify for a reward.

What to Expect

- We will acknowledge receipt of your report within 5 business days.
- We will provide regular updates on the status of your report.
- If your report qualifies for a reward, we will contact you to arrange payment.

Thank you for helping us protect our users and improve our security!