Coordinated Vulnerability Disclosure

Despite rigorous measures, we understand that vulnerabilities might sometimes occur. Thus, we extend a hand to the global community, inviting researchers to collaborate with us in identifying and rectifying any potential weak spots.

Through this policy, we aim to further consolidate our security foundations, keeping our doors open for valuable insights and fostering a safe digital environment together. This document outlines all aspects important to us when making a report to us.

Contents

Please take note of all the subjects for a thorough understanding.

Reporting Vulnerabilities

Share your findings via an email with a detailed description to security@prowise.com.

Other channels are not able to process security reports, nor can they have impact on resolutions. Please consult our contact page on our website for non-security related inquiries.

Report & Response

To expedite the resolution process, your report should ideally include:

1. **Description of the Issue:** A clear and concise description of what the vulnerability is.
2. **Steps to Reproduce:** Detailed steps to reproduce the issue, including tools or scripts used.
3. **Impact Analysis:** An analysis of the potential impact of the vulnerability.
4. **Evidence:** Screenshots, logs, or videos that substantiate the claim.
5. **Proposed Mitigation:** Optionally, suggestions for how the vulnerability can be mitigated or resolved.
6. Other relevant details that might support your case.

References

We will appreciate links to official blogs from suppliers, security professionals, relevant CVEs or OWASP documentation on the vulnerability you found to support your case. Reports with these details will enable us to make a quicker analysis of the issue and may help in correctly classifying the issue making it eligible for recognition.

Responsible Disclosure

- Do not exploit the issue beyond the extent necessary to demonstrate the vulnerability.
- Do not share the vulnerability details with others until a coordinated disclosure agreement has been established with Prowise.
- If you adhere to the guidelines mentioned in this policy, Prowise will not pursue legal actions regarding your vulnerability report.

Communication

- Prowise will acknowledge receipt of your actionable reports within 3 working days.
- We will evaluate the vulnerability and provide our assessment and planned actions within one working week.
- We commit to keeping you updated during the process of investigating and resolving the vulnerability.

Recognition

- If you wish, we will publicly acknowledge your contribution to enhancing our system's security.
- Depending on the seriousness and quality of your report, adherence to this policy, we may choose to extend you an award.

Resolution Process

At Prowise, we are committed to addressing the reported vulnerabilities swiftly and efficiently. Here's a detailed walkthrough of our response and resolution process to give you a clear understanding of what you may expect at each stage.

Acknowledgment of Receipt

Upon receiving your vulnerability report, we will:

- Send an acknowledgment of receipt within 3 working days, confirming that we have received your report and it is under review.

- Provide a unique reference number for your report, which can be used for all future communications regarding the reported issue.

Assessment and Follow-Up Actions

After the initial review, we embark on the assessment phase:

- Conduct a preliminary assessment to ascertain the severity and impact of the reported vulnerability.
- If necessary, consult with third-party security partners for an in-depth analysis and guidance.
- Develop a follow-up action plan outlining the steps to address the vulnerability, which may include immediate mitigation or scheduling a fix in a future update.

Expected Timelines at Each Stage

To maintain transparency, here are the expected timelines at each stage of the process:

- Initial Response: 3 working days to acknowledge the receipt of your report.
- Assessment and Planning: Up to one working week for a comprehensive assessment and action planning.
- Resolution: Depending on the complexity of the issue, resolution timelines may vary. We will provide an estimated timeline for resolution during the assessment phase.
- After acknowledgement, requests for updates might go unanswered if no new updates are available.

Communication Channels for Updates

Throughout the process, we will maintain open lines of communication to keep you informed:

- Progress Updates: Periodic updates on the progress of the resolution.
- Direct Communication: A direct channel for communication with our security team, utilizing the reference number provided at the acknowledgment stage.
- Public Disclosure: Coordinate with you for a mutually agreed upon public disclosure, if applicable, once the vulnerability has been resolved.

We encourage reporters to utilize the established channels for any queries or updates on the reported issues, ensuring a smooth and collaborative resolution process.

Scope of the Policy

This policy delineates the parameters and guidelines for reporting security vulnerabilities found within specific realms of Prowise's digital landscape. Adhering to these guidelines is crucial in fostering a focused collaboration to enhance our system's security. Here are the key aspects that define the scope of this policy:

In-Scope

1. Prowise's official website and all applications housed under prowise.com and related top-level domains.
2. The most recent versions of the operating system installed on the hardware products we sell.
3. The latest iterations of Prowise native applications such as Reflect, Presenter or our Chrome plugins.
4. Hardware security issues in current non-end-of-life Prowise branded hardware.

Out-of-Scope

1. Subdomains CNAMEd to a third-party system.
2. Distributed Denial of Service (DDoS) attacks and social engineering attempts.
3. Low/minimal risk issues, unless a clear and demonstrable vulnerability can be established (e.g., missing security headers that lead to an actual data breach).
4. Issues in third-party products, which should be reported directly to the concerned party unless a solution, such as modifying settings without significant loss of functionality, can be implemented by Prowise.

Vulnerability Classification

We categorize reported issues based on the likelihood of exploitation, or **probability**, and the potential technical **impact**. The classification table below illustrates how risk levels are determined:

Prb/Imp	**High**	**Medium**	**Low**	**Minimal**	**None**
High	Critical	High	Medium	Low	Minimal
Medium	High	Medium	Medium	Low	Minimal
Low	Medium	Medium	Low	Low	Minimal
Minimal	Low	Low	Low	Minimal	Minimal
None	Minimal	Minimal	Minimal	Minimal	-

Risk Descriptions

- **Critical:** Vulnerabilities that can be exploited without prerequisites and have the potential to compromise the entire system.
- **High:** Severe issues requiring prerequisites for exploitability, like access to an active user account, or resulting in high impacts such as substantial data leakage or account compromise.
- **Medium:** Difficult to exploit issues requiring in-depth system knowledge and having limited impact.
- **Low:** Issues with low risk but scope for improvement, generally enabling defense-in-depth measures.
- **Minimal:** Suggestions for improving system resilience against threats.

Dispute Resolution

In case of disputes regarding the risk score assigned to a reported vulnerability, we might consult our third-party partner for advice, which will be considered binding.

Non-actionable issues

The issues listed below are generally classified as non-actionable due to their low or minimal risk levels. However, it's important to note that the status of these issues is not set in stone; if found to be compounded with other vulnerabilities that significantly elevate their potential impact, they might be reconsidered for further investigation and action.

1. **Non-Exploitable Software Bugs:** Software bugs that cannot be exploited maliciously or do not pose any security risk.
2. **Incomplete or "Under Construction" Pages:** The presence of unfinished pages that do not expose sensitive information or functionality.
3. **Lack of Secure Flags on Non-Sensitive Cookies:** Cookies that do not contain sensitive data and are transmitted over unencrypted connections.
4. **Missing HTTP Security Headers:** Missing security headers that don't present a demonstrable security risk, such as lack of Content Security Policy headers where the risk is mitigated by other controls.
5. **Information Disclosure:** Disclosure of information like software version numbers which, on their own, do not facilitate a security breach.
6. **Rate Limiting Issues:** Issues without a demonstrable risk of abuse or exploitation, such as excessive requests to non-critical functions.
7. **Low Impact Clickjacking:** Clickjacking attacks with minimal potential impact, particularly affecting non-sensitive functionalities.

8. **Denial Of Service:** Attacks that exploit the availability of (parts of) systems when reasonable measures are already in place and working as intended.
9. **Issues with DNS:** On non-active/primary domains we may not always have all configuration as strict as it could be. These will be covered by regular internal security assessments when relevant/in scope.
10. **Cosmetic Issues:** Any visual inconsistencies or glitches which do not affect the system's security or reveal sensitive information.

We appreciate your cooperation in abiding by the scope and guidelines outlined here.

Miscellaneous

In-Scope

To streamline the reporting process, it is vital that only in-scope security issues are directed to the designated security team at Prowise. Should you have general support inquiries, these need to be addressed to service@prowise.com, where our customer service team is equipped to assist you efficiently. Please be aware that the service department is distinct from our security team and is not equipped to assist with security reports or concerns.

Status Updates

We are committed to addressing all valid security reports in a timely and thorough manner. However, due to possible resource constraints, our response time might vary. In such cases, we appreciate your patience. We kindly request that you refrain from sending high-frequency status update requests, or messages to channels other than the one outlined above for security purposes. These requests might not be fulfilled if no substantial progress has been made or new information gathered. Rest assured, our team is working diligently to investigate and respond to all reports.

Publications and Disclosures

Prowise values collaboration and transparency with the community. We are open to joint publications regarding the identified issues, provided we retain a degree of editorial control over the content to ensure accuracy and appropriateness.

Before any publication takes place, especially if vulnerabilities are still exploitable, a mutual discussion outlining a timeline and strategies for widespread adoption of fixes will be held. This collaborative approach aims to balance transparency with the responsible handling of sensitive information to safeguard our users.

Refrain from commenting on the Prowise security posture or responses publicly without our express consent or involvement. This may unintentionally create misleading expectations which we want to avoid.

Recognition

We are willing to recognize users for their valuable input, provided they have adhered to the guidelines outlined in this policy and have collaborated with us to resolve high or critical risk issues. To be eligible for recognition, contributors must supply necessary information for registration and grant us permission to publish their contribution. The acknowledgement will be featured in our Hall of Fame, with the contributors being mentioned for a period extending up to one year following the closure of the qualifying item.

Rewards

Currently, Prowise does not have a formal bug-bounty program in place. While we deeply value the diligence of external researchers, it's important to note that contributions are voluntary and do not guarantee any rewards. However, in exceptional cases where a significant vulnerability is identified, Prowise may, at its sole discretion, extend a token of appreciation. Payments shall only be done by method of choosing of Prowise.

We appreciate your understanding and urge you to comply with these guidelines. It allows us to make a quick and focused assessment of the possible threat and reward. If you do not comply with these guidelines we feel obliged to inform you that you may forfeit your right to “safe-harbor”.

Thank you for your cooperation and commitment to improving security at Prowise.

This declaration was last updated in April 2024.