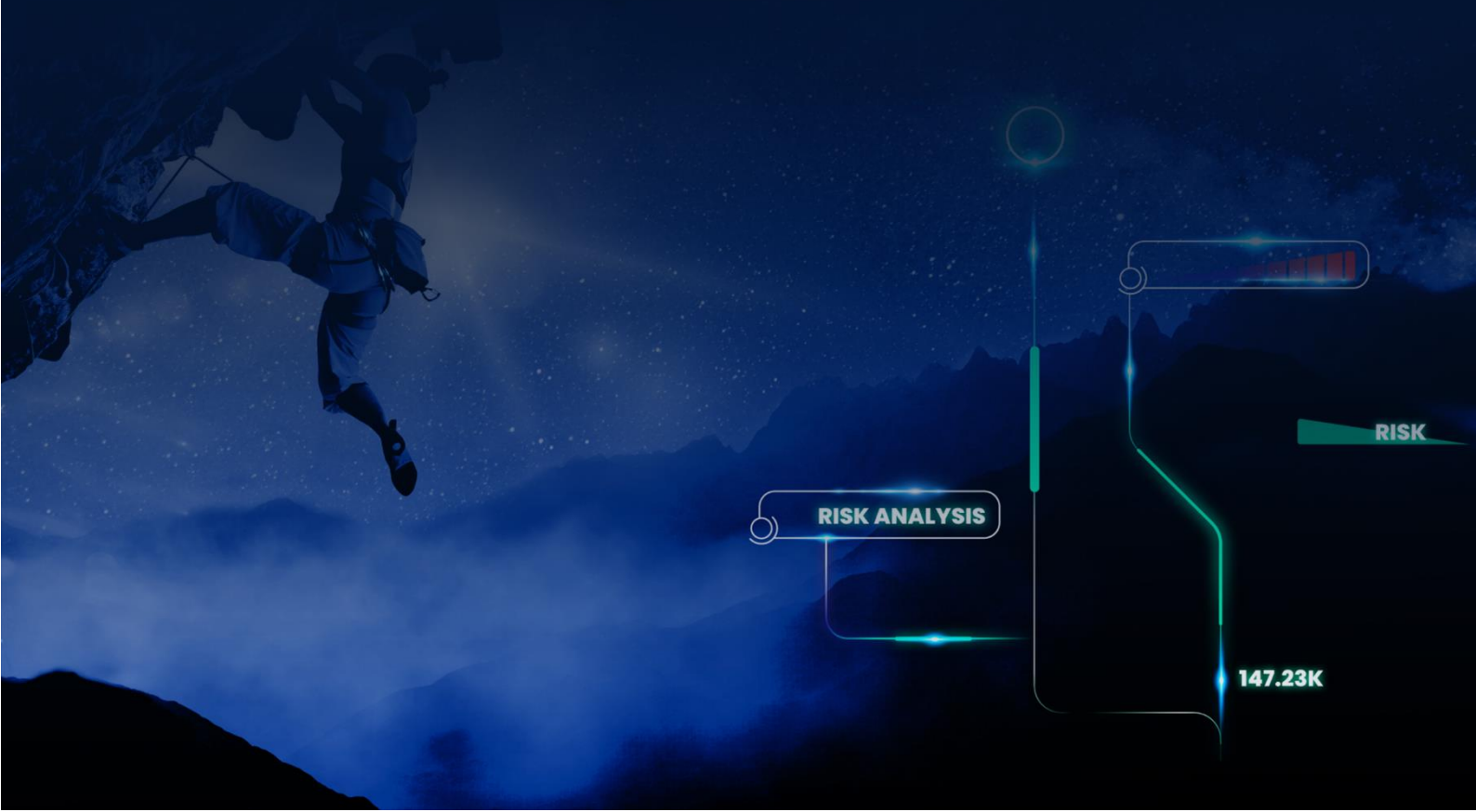
Radiflow

Vulnerability Disclosure Policy



Radiflow

Executive Summary

Radiflow is committed to securing our customers' Operational Technology (OT) networks through advanced detection and risk management strategies. To achieve this, we have implemented a comprehensive process that enhances the overall security of our products and services. This includes proactively searching for vulnerabilities, identifying and assessing them, and remediating any issues in a timely and efficient manner.

As part of Radiflow commitment to product security, we recognize the essential role of a Vulnerability Disclosure Program (VDP) in enhancing our cybersecurity and ensuring the safety of our customers. Radiflow is dedicated to working in good faith with individuals who report vulnerabilities and will officially acknowledge the contributions of the reporter.

The purpose of this policy is to provide guidelines for researchers discovering and disclosing vulnerabilities. Upon receiving a vulnerability report through our designated channels, our product and development teams will acknowledge the report, ensuring that it will undergo review promptly.

What Can You Expect?

Radiflow is committed to working with cyber researchers operating in good faith to help us enhance our overall security. As such, when reporting a vulnerability, you can expect the following from us:

- You will receive a confirmation email that your report has been received promptly.
- We will open communications with you for a better understanding of the report.
- We will provide a time frame for research and remediation of the vulnerability.
- We will keep you updated on the remediation process.
- You will be acknowledged in our official reals.

Reporting Policy

Radiflow is committed to ethical vulnerability reporting and will not pursue legal action against individuals who adhere to the Policy guidelines:

- **Safe Testing**: Engage in system testing or research without causing harm to individuals or disrupting daily activities.
- **Non-Invasive Testing**: Test products in a manner that does not affect any customers. Obtain explicit permission or consent from customers before conducting vulnerability tests on their devices, software, or systems.
- **Legal Compliance**: Ensure all testing activities comply with applicable laws and regulations.
- **Vulnerability Confidentiality**: report the vulnerability directly to Radiflow and do not disclose information on the vulnerability to any third party.

- **Privacy and Safety**: Avoid any actions that could impact the safety or privacy of Radiflow or its customers.
- **Scope**: do not exploit the vulnerability beyond confirming the vulnerability.
- **Coordinated Disclosure**: Refrain from publicly disclosing any details of the vulnerability until after a mutually agreed-upon timeframe has expired, allowing Radiflow to address the issue effectively.

Reporting Process

To report a security vulnerability affecting a Radiflow product, please contact us at psirt@radiflow.com. Radiflow typically responds to incoming reports within one business day.

To make help with the reporting process please provide with the report the following:

- A full report on the vulnerability covering where it is and how was it found.
- A step-by-step description of how the vulnerability works.
- Information regarding the testing environment.
- Any information regarding the success of exploiting the vulnerability.
- Any information that can be used to research and remediate the vulnerability.

Remediation process

After receiving a report, our team works to develop and test patches or workarounds. The duration of this process may vary depending on the complexity of the vulnerability. However, we adhere to the cybersecurity community standard timeframe of 90 days.

Disclosure and Publication process

Once a fix is available, we coordinate with the reporter on public disclosure, respecting any agreed-upon timelines to maximize protection for all stakeholders. Contributors who have helped improve our security posture are acknowledged in our advisories, receiving the recognition they deserve for their valuable input.