

Raytec Vulnerability Management Policy

Document version 1.1

INTRODUCTION

At Raytec, we are committed to delivering safe and secure products and services of the highest standards. As part of this commitment, we have established a Vulnerability Management Policy to ensure that we work diligently in handling and responding to security vulnerabilities discovered in our products.

SCOPE

The scope of this policy is to describe Raytec's vulnerability management for reporting, evaluating, and informing security vulnerabilities for all Raytec products, software and services. This policy is applicable to all [Raytec Products](#).

VULNERABILITY MANAGEMENT

We (Raytec) manage security vulnerabilities through a structured and continuous process designed to minimize threats and ensure system integrity.

When a vulnerability is identified and reported, Raytec evaluates the submission and assesses the severity of the vulnerability. Vulnerabilities are scored using the commonly known [Common Vulnerability Scoring System \(CVSS\)](#).

If a vulnerability identified is evaluated to be high/critical, we aim to resolve the vulnerability as soon as possible. Any actions taken here are properly updated to the submission.

When a vulnerability identified to be evaluated as low/medium, we may decide to resolve the vulnerability by patching the software or mitigate by disabling the functionality. Also, we may consider resolving the vulnerability as part of an upcoming release. Any actions taken here are properly updated to the submission.

HOW TO REPORT VULNERABILITIES

We investigate all reports of security vulnerabilities affecting our products and services. If you are a security researcher, partner, or end user and believe you have found a vulnerability in a Raytec product, we would like to work with you to investigate and remediate it.

If you believe that you've discovered a Security Vulnerability in one of our products, software or service, please report it directly to us through [this form](#).

The submitted report should include:

- Name of the Raytec Product or Software you believe is affected?
- Outline the vulnerability, the impact and steps to reproduce it.
- Remediation suggestion if any.

Raytec values how important your submission is, and we aim to respond within 2 business days of receiving the submission. Following that, we will provide an update on the actions we plan to take within the next 5 to 10 business days. If necessary, we may also share additional status updates. After submitting a report, you may send us a follow-up query, at any time, by emailing Security@raytecled.com.

HOW WE DISCLOSE VULNERABILITIES

For the protection of our customers, we do not disclose or discuss vulnerabilities until our investigation is complete, and a validated fix is available. Once verified, we release updates and publish details through [Product Change Notification Service](#). We encourage reporters to follow responsible disclosure practices and avoid public sharing until a fix is released.

SUBSCRIBE TO OUR SECURITY NOTIFICATIONS

At Raytec, we are committed to ensuring that you are up to date with our policies and statements on Raytec Vulnerability Management Policy. Besides, updates on this information can be obtained by subscribing to security notifications on [Raytec Security Notification Service](#).