

COULISSE

since 1992

RESPONSIBLE DISCLOSURE POLICY

Introduction

At Coulisse, we consider the security of our systems very important. Despite the attention and care we give to the security of our systems, there may still be weak spots in our systems.

If you notice a vulnerability, we encourage you to let us know. We would like to hear from you so that we can take appropriate action immediately. This way, we will work together to fix the problems and make our systems even more secure.

How to report?

A notification can be addressed to security@coulisse.com.

When making a report, we would like to ask you for sufficient and clear information so that we can properly identify the problem. We are especially curious to know how the security problem could be abused. Preferably explain this with an explanation and possibly with screenshots. Also mention the date and time you found the problem. This helps us to analyse the problem and find a suitable solution as quickly as possible.

We would also like to receive your contact details so that we can communicate with you about the report. Would you rather not? Then you can also choose to make the report anonymously.

Important points we would like to ask and impress upon you

- Do not make the vulnerability public or share it with others.
- Do not abuse the problem by, for example, copying, modifying or deleting data, posting a malware or downloading more data than necessary to demonstrate the problem.
- Delete all confidential information obtained through the vulnerability found immediately after the problem is fixed.
- Do not run tests that use physical security attacks, social engineering, (Distributed) Denial of Service or third-party applications.
- Do not use 'Brute Force Attacks' to get into our systems.

What you can expect from us

After you file the report, you will receive an acknowledgement of receipt as soon as possible. If you have not made the report anonymously, we will do our best to contact you about the report within 5 working days and will keep you informed about the progress of solving the problem. Coulisse's Cyber Security Engineer will deal with the report; he will analyse the vulnerability found and try to come to an appropriate and suitable solution.

Coulisse will treat your report confidentially. Your details will not be shared without your permission and your contact details will only be used to communicate with you about the report. An exception to this is if we are required by law to share your details or if we suspect that you are not acting in good faith and are guilty of a criminal offence.

If coverage of the reported security problem will appear, we will, with your permission, include your name as the discoverer. Of course, you can also choose to remain anonymous if you prefer.

COULISSE

since 1992

Reward

As a thank you for your help and helping us better protect our systems, we would like to reward you for reporting a security problem still unknown to us. The reward depends on the severity of the vulnerability and the quality of the report.

We additionally offer rewards only for reports that meet the conditions below:

- The notification must contain a sufficiently clear and detailed description of the security problem.
- While investigating the vulnerability, no damage should be done to our systems.
- The vulnerability must be new to us. Reports of problems previously reported or already known to us are not eligible for a reward.

Legal position

Coulisse will not take any legal action against you as reporter of the security problem. The condition for this is that you have acted in good faith and in the spirit of 'responsible disclosure'. If we suspect that you are guilty of a criminal offence, we will report you to the police.