Introduction

The CAR 2 CAR Communication Consortium (C2C-CC) aims at assisting towards accident free traffic (vision zero) at the earliest possible date. It further aims at supporting the highest safety level at improved traffic efficiency anywhere, anytime at the lowest cost to the end user and the environment. While working on solutions supporting all driving levels from manual to fully automated it considers specific needs of stakeholders, types of vehicles and users. The C2C-CC contributes to the development and specification of robust and reliable solutions that allow for a continuous and seamless evolution of required functionalities. It enables technologies driven by innovation and competition, thereby fostering concepts of cooperation between the road users and with the road infrastructure. This is based on sharing information, awareness, perception and intentions while focusing on tactical level and considering strategic and planning level as required.

This vulnerability disclosure policy applies to any vulnerabilities you are considering reporting to us (the
C2C-CC). We recommend reading this vulnerability disclosure policy fully before you report a vulnerability and
always acting in compliance with it.
We value those who take the time and effort to report (security) vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures.

Reporting

If you believe you have found a (security) vulnerability, please submit your report to us using the following webform:

- https://www.car-2-car.org/webform-first-contact

Please fill in the fields as they are marked as mandatory or optional.
I case you are reporting a security vulnerability, pleas tick the according field. Which will allow you to submit the information anonymously. For technical vulnerabilities, contact information are mandatory, so that we can get in touch with you in case further clarification of the report would be needed or to give you feedback about the handling of vulnerability.

What to expect

After you have submitted your report, we will respond to your report within 5 working days and aim to triage your report within 10 working days. We will also aim to keep you informed of our progress.
Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation.
We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately.

Guidance

Do NOT:

- Break any applicable law or regulations
- Access unnecessary, excessive or significant amounts of data
- Modify data in the Organization's systems or services
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities
- Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests
- Disrupt the Organization's services or systems