

ECO3 Vulnerability Disclosure Policy

Version: 1.0

Last Reviewed: September 2026

1. Introduction

At ECO3, we consider the security of our products, applications, websites and digital services to be an important responsibility.

While we continuously work to improve security, vulnerabilities may still exist. If you discover a potential security vulnerability affecting ECO3, we would like to hear about it so that we can investigate, assess and take appropriate action.

This Vulnerability Disclosure Policy explains how potential vulnerabilities may be reported to ECO3 and how ECO3 will handle such reports.

2. How to report a vulnerability

This policy applies to products, applications, websites and digital services owned, developed, maintained or made available by ECO3.

For the avoidance of doubt, this policy also applies to vulnerabilities affecting third-party software, open-source software, libraries, frameworks or other components that are integrated into, distributed with, or otherwise form part of ECO3 products, applications or services.

This policy does not apply where the reporter is subject to separate contractual obligations, including under a non-disclosure agreement, beta testing agreement, evaluation agreement or similar arrangement with ECO3 or its affiliates.

This policy allows vulnerabilities to be reported to ECO3, but it does not provide general authorization to perform security testing. Systems, products or services not owned or operated by ECO3 are outside the scope of this policy

Potential vulnerabilities may be reported to:

security.team@eco3.com

If possible, please send us a PGP-encrypted email using the following:

- [PGP KEY](#)
- Fingerprint: 3798 8BC7 533C E808 9CF0 4095 D09C 6A62 B7E6 611D

To help speed up investigation and coordination, ECO3 prefers vulnerability reports to be submitted in English.

To assist our investigation, please provide as much information as possible, including:

- a description of the vulnerability
- the affected product, application, website or service;
- the affected version(s), where known;
- the potential impact;
- steps required to reproduce the issue;
- suggested mitigations, if available.

To support effective investigation and coordination, reporters are requested to indicate, where known:

- whether the vulnerability has already been disclosed to any external party, publicly or privately;
- whether the vulnerability is known or suspected to be under active exploitation;
- whether any public references, advisories or vulnerability identifiers are associated with the reported issue.

Reporters should limit submitted information to what is reasonably necessary to describe and reproduce the issue. Where possible, reporters should avoid including personal data, confidential information, proprietary information or other sensitive content in vulnerability reports, screenshots, recordings or supporting materials. If such information is encountered during testing, reporters should immediately cease testing and notify ECO3. Vulnerability reports will be processed solely for the purpose of assessing, investigating, mitigating and remediating security issues and complying with applicable legal obligations.

3. Expectations for reporters

ECO3 requests that reporters:

- act with the objective of improving security;
- do not perform activities that could negatively impact service availability;
- avoid accessing, modifying, deleting, copying or disclosing data that is not their own;
- immediately cease testing and notify ECO3 if personal data, confidential information or other sensitive information is encountered;
- do not perform social engineering, physical attacks or similar activities;
- do not use automated tools or techniques that could significantly affect the availability, integrity or performance of systems;
- keep information relating to the vulnerability confidential at least until ECO3 has completed its initial assessment and had an opportunity to implement appropriate mitigation measures.
- cooperate with ECO3 during the assessment of a reported vulnerability, including by providing additional information, clarification or reasonable assistance where necessary to enable ECO3 to understand, reproduce, validate or remediate the reported issue.

4. Our commitment

Upon receiving a vulnerability report, ECO3 will:

- review the information provided;
- assess the validity and potential impact of the reported vulnerability;
- coordinate investigation and remediation activities as appropriate;
- request additional information where necessary;
- seek to manage vulnerabilities through a coordinated disclosure approach.

ECO3 will make reasonable efforts to acknowledge vulnerability reports and, where reasonably practicable, provide updates regarding the progress of its investigation.

ECO3 does not guarantee specific response, remediation or disclosure timelines.

By reporting potential security vulnerabilities in accordance with this Policy, you can do so with the confidence that ECO3 will not pursue legal action against you solely for identifying and reporting the vulnerability.

This protection does not apply to activities that:

- violate applicable laws or regulations;
- compromise confidentiality, privacy, data integrity or service availability;
- cause harm to ECO3, its customers, employees, partners or other parties;
- involve extortion, threats or requests for payment.

5. Coordinated vulnerability disclosure

ECO3 supports coordinated vulnerability disclosure and believes vulnerabilities should be addressed in a manner that reduces risk to customers and other stakeholders.

ECO3 requests that reporters provide ECO3 with an opportunity to investigate, validate and, where appropriate, remediate reported vulnerabilities before public disclosure.

Where required by law, or where reasonably necessary to investigate, assess, mitigate, remediate or coordinate the handling of a reported vulnerability, ECO3 may share information contained in vulnerability reports, including technical details and supporting materials, with appropriate parties involved in the handling of the vulnerability.

Such parties may include, among others, service providers, suppliers, maintainers, developers, advisors, customers, competent authorities or other parties whose involvement is reasonably necessary to assess or address the vulnerability.

ECO3 will seek to limit such disclosures to information reasonably necessary for those purposes.

This text is a derivative work of "Responsible Disclosure" by Floor Terra, used under a Creative Commons Attribution license 3.0.