

Document	Vulnerability Disclosure Policy						
Doc. Name* ¹	Vulnerability Disclosure policy 1.0.docx						
Version* ²	1.0	Status* ²	Approved	Effective	06-11-2024	¹ Update: Double click right mouse choice " update field" ² Draft=0,1,1,../Released = 1,0, 2,0../Obsolete = latest version	

*¹ Update: Double click right mouse choice "update field"
*² Draft=0.1, 1.1.../Released = 1.0, 2.0.../Obsolete = latest version

Revision history

Rev. Number	Description of change	Name	Date
0.1	Draft version	Johan Immink	08-03-2024
0.2	Updated and translated in English	Natasha Pasricha	18-06-2024
1.0	Approved version	Natasha Pasricha	06-11-2024

Purpose and scope

The purpose is to encourage collaboration between customers or cybersecurity community and organizations. This will ensure early detection of vulnerabilities by providing a clear and structured way for security researchers and ethical hackers to report vulnerabilities they discover, ensuring that such information reaches the right people within the organization.

References

Ref	Doc ID	Document title
[R1]		
[R2]		

Definitions

Term	Definition

1 Vulnerability Disclosure Policy

At CowManager, we prioritize the security of our systems, network, and products. Despite our best efforts to maintain high security standards, vulnerabilities may still be discovered. If you identify a vulnerability, we ask that you report it to us as soon as possible so we can take prompt action.

1.1 Discovery of Vulnerabilities

Vulnerabilities can be found in two ways:

1. Accidental discovery during normal use of a digital environment.
2. Deliberate attempts to find vulnerabilities.

1.1.1 Scope and Approach

Our vulnerability disclosure policy is not an invitation to extensively scan our corporate network for vulnerabilities. We manage our own network monitoring.

Products: You are encouraged to actively search for vulnerabilities in offline, non-production environments and online, cloud environment and in the (web) app. Please report any findings to us. While we discourage hacking attempts on our customers' infrastructure, we still request that any discovered vulnerabilities be reported to us promptly so we can address them.

Document	Vulnerability Disclosure Policy						
Doc. Name* ¹	Vulnerability Disclosure policy 1.0.docx						
Version* ²	1.0	Status* ²	Approved	Effective	06-11-2024	¹ Update: Double click right mouse choice "update field" ² Draft=0.1, 1.1.../Released = 1.0, 2.0.../Obsolete = latest version	

1.1.2 Collaboration

We aim to collaborate with security researchers and ethical hackers from cybersecurity communities to enhance security, for our organization and of our products and our services.

1.1.3 Reporting Guidelines

Please follow these guidelines when reporting a vulnerability:

- **Report Promptly:** Email your findings as soon as possible to incident@cowmanager.com
- **Avoid Misuse:** Do not exploit the vulnerability by downloading, altering, or deleting data. We will take your report seriously and investigate all suspected vulnerabilities, even without concrete proof.
- **Confidentiality:** Do not share the vulnerability with others until it is resolved.
- **Ethical Conduct:** Avoid using attacks on physical security, social engineering, or hacking tools like vulnerability scanners.
- **Detailed Reporting:** Provide sufficient information to reproduce the problem. Typically, an IP address or URL of the affected system and a description of the vulnerability are enough. More details may be needed for complex issues.

1.2 Our Commitments

- **Timely Response:** We will respond within 5 business days with our assessment and an expected resolution date.
- **Confidentiality:** Your report will be treated confidentially. We will not share your personal information with third parties without your permission, except for law enforcement if required.
- **Progress Updates:** We will keep you informed of the progress in resolving the issue.
- **Acknowledgment:** If you wish, we will credit you as the discoverer in any communication about the reported problem.
- **Legal Considerations:** We will assess each situation individually. We are morally obligated to report to law enforcement if we suspect misuse of the vulnerability or data, or if you share knowledge of the vulnerability with others. Accidental discoveries in our online environment will not lead to legal action.
- **Rewards:** We offer a reward for reporting unknown security issues. The reward amount is based on the severity of the vulnerability and the quality of the report. We strive to resolve all issues quickly, keep all parties informed, and participate in any publication about the problem once resolved.

Thank you for helping us improve our security. Your efforts contribute to the safety of our customers and systems.

--End of the document--