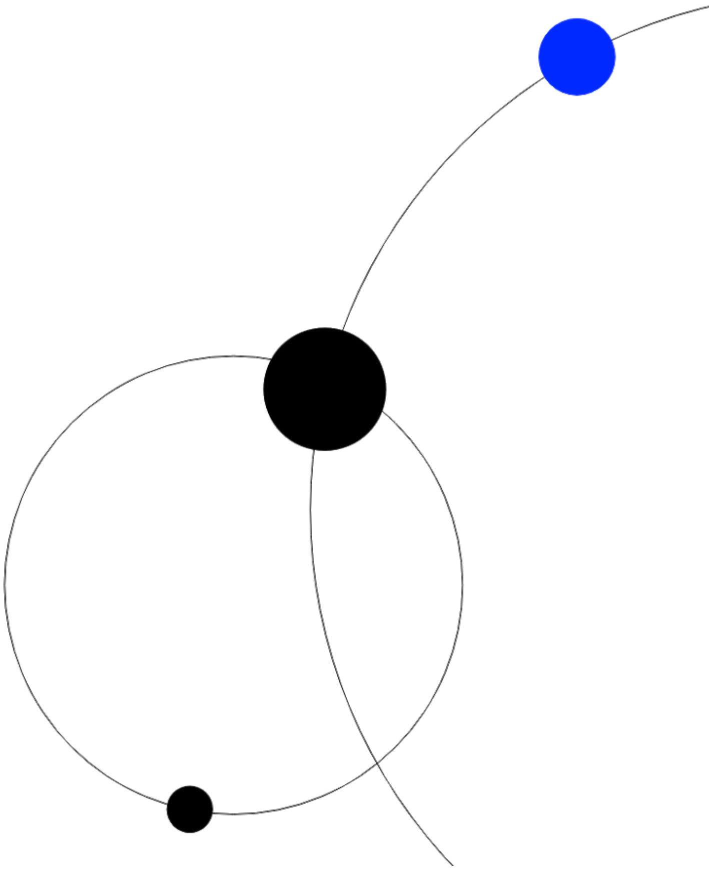
celonis



Vulnerability Disclosure Program

Execution Management System

Introduction

Thank you for taking interest in the security of Celonis. We recognize the value security researchers and security experts can provide to our organization acting in good faith to help us maintain a high standard for the security and privacy of our platform.

Expectations

When working with us according to this policy, you can expect us to:

- Work with you to understand and validate your report, including a timely initial response to the submission.
- Work to remediate discovered vulnerabilities in a timely manner.
- Recognize your contribution to improving our security if you are the first to report a unique vulnerability, and your report triggers a code or configuration change.

Targets

Included:

https://snap-*.eu-1.celonis.cloud

https://*.training.celonis.cloud

Excluded:

*.celonis.com

*.celonis.de

*.celonis.cloud

Out of scope

- Descriptive error messages (e.g. stacktraces, application or server errors)
- Lack of rate limit on non-sensitive endpoints and/or brute force attacks
- Clickjacking/UI redressing with no practical security impact
- Presence of application or web browser 'autocomplete' or 'save password' functionality
- Logout Cross-Site Request Forgery (logout CSRF)
- Missing cookie flags on non-sensitive cookies
- Open ports that do not lead directly to a vulnerability
- Login or Forgot Password page brute force and account lockout not enforced
- OPTIONS / TRACE HTTP method enabled
- Lack of the X-FRAME-OPTIONS header
- SSL/TLS best practices
- Presence/absence of SPF / DMARC records
- Self XSS
- Internal IP disclosure
- Vulnerabilities that require extensive social engineering
- The Anti-MIME-Sniffing header X-Content-Type-Options
- Missing HTTP security headers
- Functional, UI, and UX bugs and spelling mistakes
- Physical attacks on Celonis infrastructure or facilities
- DoS/DDoS or any other testing that would impact the operation of our systems
- Social engineering attacks or phishing
- Testing third-party applications or services
- Subdomain takeover without taking the subdomain over
- Vulnerabilities only affecting users of outdated or unpatched browsers and platforms

Rewards

- Celonis Security Bounty payments are granted solely at the exclusive discretion of Celonis.

Program Rules

To encourage vulnerability research and to avoid any confusion between legitimate research and malicious attack, we ask that you attempt, in good faith, to:

- Play by the rules. This includes following this policy any other relevant agreements.
- Perform testing only on in-scope systems, and respect systems and activities that are out-of-scope.
- Avoid violating the privacy of others, disrupting our systems, destroying data, and/or harming user experience. Actions that affect the integrity or availability of program targets are prohibited and strictly enforced. If you notice performance degradation on the target systems, you must immediately suspend all activities. This includes attacking any accounts other than your own and using phishing or social engineering techniques.
- Never use a finding to compromise/exfiltrate data or pivot to other systems. Use a proof of concept only to demonstrate an issue.
- Do not engage in extortion.
- Testing should be performed only on systems listed under the program brief 'Targets' section. Any other systems are Out Of Scope.
- Submissions must be made exclusively through **security-bugs@celonis.com**. You can optionally encrypt all communications with the Celonis PGP Key. Include all relevant videos, crash logs, and system diagnosis reports in your email.
- The report cannot be made public unless there is explicit authorization by Celonis.
- Submissions may be closed if a researcher is non-responsive to requests for information after 7 days.

Report Guidelines

- Submission reports should include:
    - A detailed description of the issues being reported.
    - Any prerequisites and steps to get the system to an impacted state.
    - A reasonably reliable exploit for the issue being reported.
    - Enough information for Celonis to be able to reproduce the issue.
    - We encourage researchers to include a video or screenshot Proof-of-Concept in their submissions. These files should not be shared publicly. This includes uploading to any publicly accessible websites (i.e. YouTube, Imgur, etc.).

Safe Harbor

Participants must feel that disclosure would not subject them to penalties to facilitate the research to be conducted under this policy. Therefore, one of the most critical components of this policy is a clear, unambiguous commitment that good faith efforts in accordance with this policy will not result in Celonis initiating legal action. Any activities conducted in a manner consistent with this policy will be considered authorized conduct, and Celonis will not initiate legal action against such Participants. In general, Celonis' goal is to create a "safe harbor" that demonstrates good faith and builds trust. Celonis cannot authorize efforts on third-party products or guarantee that third parties do not pursue legal action against a Participant. However, if a third party threatens or brings any legal action against the Participant for his/her efforts under this policy, Celonis is willing to make clear - to the court, the public, or otherwise - that Celonis authorized the Participant's efforts to test and research the security of Celonis' eligible systems and services.