revevol | The Game Changer in Cloud Business

Harbor Vulnerability Disclosure Program

Table of contents

Disclosure

This vulnerability disclosure program is limited to security vulnerabilities in “Harbor” web application owned by Revevol. This program does not provide monetary rewards.

Eligible Vulnerabilities

We consider a security vulnerability to be a weakness in our product or infrastructure that could allow an attacker to impact the confidentiality, integrity, or availability of the product or infrastructure as for example:

Vulnerabilities by Category

- **Access Controls**: related to authorization of users, and assessment of rights.
- **Auditing and Logging**: related to auditing of actions, or logging of problems.
- **Authentication**: related to the identification of users.
- **Configuration**: related to security configurations of servers, devices, or software.
- **Cryptography**: related to mathematical protections for data.
- **Data Exposure**: related to unintended exposure of sensitive information.
- **Data Validation**: related to improper reliance on the structure or values of data.
- **Denial of Service**: related to causing system failure.
- **Error Reporting**: related to the reporting of error conditions in a secure fashion.
- **Patching**: related to keeping software up to date.
- **Session Management**: related to the identification of authenticated users.

Detailed vulnerabilities:

- **Cross-site scripting**
- **Cross-site request forgery in a privileged context**
- **Server-side code execution**
- **Authentication or authorization flaws**
- **Injection Vulnerabilities**
- **Directory Traversal**
- **Information Disclosure**
- **Significant Security Misconfiguration**

How to report a Vulnerability

Any vulnerabilities you may find should be reported via email to our Product Security Incident Response Team via an email sent to the following address: harbor-security@revevol.eu. To ensure confidentiality, we encourage you to encrypt any sensitive information you send to us via e-mail.

We expect reports in English providing clear and concise steps to reproduce the issue and by including the following information:

- Time and date of discovery
- URL, browser information including type and version and input required to reproduce the vulnerability;
- Technical Description — provide what actions were being performed and the result in as much detail as possible;
- Sample Code — if possible, provide code that was used in testing to create the vulnerability;
- Reporting's party Contact Information — best method to reach
- Threat/Risk Assessment — contains details of the identified threats and/or risks including a risk level (high, medium, low) for assessment result;
- Software Configuration — details to computer/device configuration at time of vulnerability;
- Relevant information about connected devices if vulnerability arises during interaction. When a secondary device triggers the vulnerability, these details should be provided.

Please do not include personal data in your reports, except what is necessary for us to contact you.

Terms and Conditions

- Please use your own account for testing or research purposes. Do not attempt to gain access to another user's account or confidential information.
- Please do not test for spam, social engineering or denial of service issues.
- Your testing must not violate any law, or disrupt or compromise any data that is not your own.
- Participating in this program does not give you any right to intellectual property owned by Revevol or any third party.

- By submitting a report to us, you warrant that the report and any attachments do not violate the intellectual property rights of any third party and you grant us a non-exclusive, royalty-free, world-wide, perpetual license to use, reproduce, create derivative works, and publish the report and any attachments.
- Revevol retains discretion to determine whether to accept a report into the program. For example, Revevol will not accept into this program vulnerabilities with minimal security impact or low exploitability, vulnerabilities beyond Revevol's control, vulnerabilities discoverable through automated scans which have not been verified manually, or vulnerabilities related to a violation of the program requirements.
- The harbor-security@revevol.eu email address is intended ONLY for the purposes of reporting product or service security vulnerabilities. It is not for technical support information on our products or services. All content other than that specific to security vulnerabilities in our products or services will not be processed.
- The reporting party(s) who submits a report to Revevol through this program agrees not to disclose to a third-party any information related to that report, the vulnerability reported, nor the fact that a vulnerability has been reported to Revevol. This agreement regarding disclosure applies regardless of whether Revevol had prior knowledge of the information. If you believe others should be informed of the vulnerability prior to our implementation of corrective actions, we require that you coordinate in advance with us.
- All aspects of this program are subject to change without notice, as well as to case-by exceptions. No particular level of response is guaranteed for any specific issue or class of issues.