Proprietary and Confidential

Vulnerability Research and Responsible Disclosure Policy

Updated 24 August 2023

Product Security

Habanero Systems values the work done by a security researcher in improving the security of our products and service offerings. We are committed to verifying and reproducing legitimate reported vulnerabilities within this community. We encourage the community to participate in our responsible reporting process.
If you are a security researcher or ethical hacker and would like to report a security vulnerability, please email disclosure@habanerosystems.com

With each report, you will need to provide contact information and company name (If applicable).

Note: Failure to adhere to the Responsible Disclosure Guidelines and contact us through the appropriate channels outlined in this guide will result in your request being treated as spam.

Responsible Disclosure Guideline

We will investigate legitimate reports and try to correct any vulnerabilities quickly. To encourage responsible reporting, we commit that we will not take legal action against you if you comply with the following:

- You must include sufficient information, including details of vulnerabilities and knowledge we will need to reproduce the vulnerabilities.
- Make a reasonable effort to avoid privacy violations, data destruction, and interruption or degradation of our services.
- Please do not make any changes or access our database that does not belong to you.
- Allow us reasonable time to correct the issue before publicizing any information.
- We will attempt to respond to your report within 3 - 5 Days.

Services in Scope

Any data or subsidiary web service hosted by Habanero Systems that handles sensitive user data is within the scope, which includes all the content in the following domains:
*.insvr.com
*.habanerosystems.com

Services that are not within the scope

Third-party websites. Our vendors or partners operate some Habanero Systems services hosted. We can't authorize you to test these systems on behalf of their owners and will not reward such reports. If in doubt, talk to us first!
Recently created or acquired. To allow time for internal review and remediation, newly acquired or created domains and services are subject to a six-month blackout period. Bugs reported sooner than that will typically not qualify for a reward.
Qualifying vulnerabilities
Any design or implementation issue that substantially affects the confidentiality or integrity of user data is likely in the program's scope. Common examples include:

- Cross-site scripting,
- Cross-site request forgery,
- Mixed-content scripts,
- Authentication or authorization flaws,
- Server-side code execution bugs.

Please note that the program's scope is limited to technical vulnerabilities in Habanero Systems-owned services and web applications.

Legal points

We cannot issue rewards to individuals on sanctions lists or who are in countries (e.g., Cuba, Iran, North Korea, Syria, Crimea, and the so-called Donetsk People's Republic and Luhansk People's Republic) on sanctions lists.
You are responsible for any tax implications depending on your country of residency and citizenship.
In addition, depending on your local law, additional restrictions on your ability to enter may exist.
And your testing must not violate any law or disrupt or compromise any data that is not yours. It would be best if you understood that we could cancel the program at any time and the decision as to whether to pay a reward has to be entirely at our discretion.