Vulnerability Disclosure Policy

As the vendor of BlueSpice, Hallo Welt! GmbH takes the security of its systems seriously, and we value the security community. The disclosure of security vulnerabilities helps us ensure the security and privacy of our users. If you believe you have found a vulnerability or security issue in one of our Hallo Welt! products, we appreciate a report with the related details. Before reporting a security issue, please read our disclosure policy on how we handle security related bugs and issues.

For a list of known security issues, please see our **Security Advisory** list.

Guidelines

We kindly ask that all researchers:

- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction of data during security testing.
- Perform research only within the scope set out below.
- Use the identified communication channels to report vulnerability information to us.
- Keep information about any vulnerabilities you've discovered confidential between yourself and Hallo Welt! GmbH until we've had 90 days to resolve the issue.
- Not ask for payments. We are a small company, and might reward someone if an issue with significant impact is found, but we do not promise any monetary reward. We only promise to add your name to Hall of Fame page if the issue is confirmed as valid.

If you follow these guidelines when reporting an issue to us, we commit to:

- Not pursue or support any legal action related to your research.
- Work with you to understand and resolve the issue quickly (including an initial confirmation of your report within 1 week of submission).
- Recognize your contribution on our **Security Researcher Hall of Fame**, if you are the first to report the issue and we make a code or configuration change based on the issue.

Scope

The main scope of this policy is the development of our software BlueSpice and its deployment in various environments:

- BlueSpice on premise
- BlueSpice Docker
- BlueSpice Cloud
- BlueSpice documentation and demo instances

The following versions of BlueSpice are currently being supported with security updates:

- The current minor version of BlueSpice.
  See **https://en.wiki.bluespice.com/wiki/Setup:Release_History**

Furthermore, we value reports about security issues in:

- All repositories maintained by Hallo Welt!
- All services operated by Hallo Welt!

Out of Scope

Any services hosted by 3rd party providers.

Unsupported versions of BlueSpice (see above)

Security issues related to MediaWiki or any 3rd party libraries we build upon. If you find such security issues, please report directly to the appropriate vendors. If in doubt, talk to us and we will point you to those vendors if applicable.

In the interest of the safety of our users, staff, the Internet at large and you as a security researcher, the following test types are excluded from scope:

- Findings from physical testing such as office access (e.g. open doors, tailgating).
- Findings derived primarily from social engineering (e.g. phishing, vishing).
- Findings from applications or systems not listed in the 'Scope' section.
- UI and UX bugs and spelling mistakes.
- Network level Denial of Service (DoS/DDoS) vulnerabilities.

If you are unsure whether something is out of scope, feel free to contact us via **security@bluespice.com**.

How to report a security vulnerability

If you believe you've found a security vulnerability in one of our products or platforms, please send it to us by emailing **security@bluespice.com**. Please include the following details in your report:

- Description of the location and potential impact of the vulnerability.
- A detailed description of the steps required to reproduce the vulnerability (POC scripts, screenshots, and screen captures are all helpful to us).
- Your name/handle and a link for recognition in our Hall of Fame.

If you'd like to encrypt the information, please use our **PGP key**.

After receiving the report, Hallo Welt! will

- request the reporter to keep the information and communication of the vulnerability confidential.
- verify the existence of the vulnerability and identify which releases are affected. When confirmed, we will assign a CVE ID to the issue, if applicable.
- release an updated version of the affected products resolving the issue as soon as possible. If it is not possible to resolve the issue within a reasonable time frame, identified workarounds might be published if that improves the situation in an acceptable way without putting users at risk.
- include a reference to the reporter and/or its organization to its **Security Researcher Hall of Fame**, unless the reporter wishes to remain anonymous.
- do its best to keep the reporter updated on the progress of the reported vulnerability.
- publish a **security advisory** after resolution of the issue.