Security Policy

Thanks for helping make Parsec safe for everyone.

We take the security of our software products and services seriously, including all of the open source code repositories managed through our GitHub organization, Scille.

If you believe you have found a security vulnerability in any Scille-owned repository, please report it to us through coordinated disclosure as described below.

Disclosure policy

Please do not report security vulnerabilities through public GitHub issues, discussions, or pull requests.

Instead, please send an email to security@parsec.cloud.

Include as much of the information listed below as you can to help us better understand and resolve the issue:

- The type of issue (e.g., buffer overflow, SQL injection, or cross-site scripting)
- Full paths of source file(s) related to the manifestation of the issue
- The location of the affected source code (tag/branch/commit or direct URL)
- Any special configuration required to reproduce the issue
- Step-by-step instructions to reproduce the issue
- Proof-of-concept or exploit code (if possible)
- Impact of the issue, including how an attacker might exploit the issue

This information will help us triage your report more quickly.

Security Update Policy

When the security team receives a security bug report, they will assign it to a primary handler. If the issue is confirmed, this person will coordinate the fix and release process, involving the following steps:

- Determine the affected versions.
- Audit code to find any potential similar problems.
- Prepare fixes for all releases still under maintenance.

These fixes will be released as soon as possible depending on complexity.