Coordinated Disclosure Policy

Version 1.2, last updated: April 22, 2020

We do our best to make sure our software is free of any security vulnerabilities. The reality though is that it's not always the case. That is why we are very eager and grateful to hear about any issues you find.

Where to report issues

Please report these issues

- Directly to our issue tracker (setting issue type to 'Security Problem' to limit visibility).
- Via email encrypted with a PGP key, you can find this on most public key servers.

Scope

Reported issues should be related to

- JetBrains products, or
- JetBrains websites

Reporting conditions

Those reporting issues should conform to the following conditions:

- All communication and disclosure should be made in a coordinated manner, not putting our business or our users and customers at risk.
- The issue should contain a description and working proof of concept.
- There should not be any attacks that attempt to access JetBrains or our customers' confidential data.
- There should not be any attacks that lead to denial of service attacks on our systems and services or jeopardizing them in any way.
- No automated tools should be used for attacking our systems or services.
- No social engineering should be targeted against JetBrains employees or customers.

Proof of concept

- Proof of concept should be drafted using your data when possible.
- The impact from the demonstration should be limited to the necessary minimum required to prove the concept.
- Where it is not possible to avoid interacting with real users or their data, the impact should be minimized to a few entries where it is absolutely necessary to demonstrate a vulnerability.
- The confidentiality, integrity, and availability of our products, services, data, and business processes are to be respected.

Bug Bounty

We don't have a formal bug bounty program but depending on the severity of an issue, we often reward reporters based on the issue's score according to CVSS. The issue should not already have been announced publicly or known by JetBrains. This includes issues that we are aware of but have not yet disclosed publicly for whatever reasons.

Timeline

- As soon as possible
  - Triage reported vulnerabilities as soon as possible depending on their impact.
  - Prevent further exposure of users data and further exploitation of a security issue.
- 24 hours from receiving the report
  - Respond to your report with a confirmation of receipt and any questions, or an update on the planned course of action.
- With next release or bug fix update
  - We release updated products with security fixes with the next release or bug fix update.
  - Shortly after that we inform our customers about the vulnerability and recommend that they update to a more secure version of the product.
- Weeks following
  - Announce the vulnerability and its fix on the JetBrains Blog or the product blog. The exact number of weeks depends on multiple factors including planned time for our customers to update their software if necessary.
- Following quarter
  - Announce vulnerabilities we've fixed over the past quarter in our Security Bulletin that you can subscribe to.

If you have any questions or concerns regarding this policy, please reach out to security@jetbrains.com.