Security Issues and How to Report Them

MetaSlider Security · https://www.metaslider.com/docs/security-issues-and-how-to-report-them/

We do our best at MetaSlider to solve all security issues. We aim to develop, test, release and announce patches as quickly as possible after issues have been discovered.

Full details are available to customers and other trusted parties on request.

How to report a security issue

If you have discovered a vulnerability in a MetaSlider plugin, we want to hear from you as soon as possible.

Please gather as much information together as you can so we can work quickly to address it. Here's a checklist of the details we'd like to see.

1. Severity (high, medium, low)
2. Vulnerability type: e.g., DoS, Overflow, XSS, CSRF, etc
3. Exploitation Requires Authentication?: yes/no
4. Which plugin is vulnerable and which version numbers.
5. A description of the vulnerability
6. Do you have reason to believe the vulnerability is being exploited?
7. Are details of an exploit publicly available? If so, please provide us with a URL.
8. What is the potential impact? How do you envisage it being used in an attack scenario?
9. DREAD score, if known.
10. CVE Identifier / Reference / Advisory Number, if applicable.
11. If you wish to be credited for the responsible disclosure in the release announcement and the change log, please let us know. If you plan to disclose details of the vulnerability, please do let us know so we can coordinate the timing of the disclosure together.
12. Any additional comments.

If you are a customer please open a support ticket as soon as possible and make it clear in the subject that you are reporting a security vulnerability.

If you are not a customer, send all the details to **security@metaslider.com**.

We will acknowledge receipt as soon as we've read it. If we don't acknowledge your email quickly, please assume we have not received it and re-send.

If the issue is confirmed, we'll plan a patch and let you know when we plan to release it.

Responsible disclosure of issues

Sometimes security researchers have contacted us to disclose a security vulnerability. In these cases, it's understandable that the researcher might want to publish details of the discovery themselves.

We do expect researchers to respect the principles of responsible disclosure and to work with us to coordinate the content