Responsible disclosure

Astaria's Responsible Disclosure Program Reports should be submitted via email to security@astaria.xyz . Reports may be submitted anonymously and/or encrypted per instructions below.

- All bug reports must be fixed and paidBEFORE
- being published.
- Whitehats may NOT publish information about reports rejected as being a duplicate or known issue.
- Whitehats may NOT publish information during the mediation process.
- Bug report intellectual property remains with the whitehat. Right of publication, however, is determined by whichever publication category the project chooses.
- Astaria will investigate legitimate reports and make every effort to quickly resolve any vulnerability. Please make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our services.
-

Note that Astariarequires notice prior to publishing any findings:

- Whitehats may publish information about their fixes and paid bug reports provided that they give projects 21 days to review and provide input about the publication in the bug report submission thread before they publish.
- Whitehats do NOT need to provide notice prior to publishing information about payment amount, severity, or high-level classification of the bug type (e.g. reentrancy), as long as they do not mention or indicate the project to which it was reported.
- The notice requirement does NOT apply to Whitehats publishing information about reports that have not been resolved within 90 days of escalation, unless a mediation process is ongoing. In those instances, the Whitehat may disclose information pertaining to that bug report without restriction.
-

If you have any questions or concerns about about Astaria's disclosure policy, please contact us via Twitter , Discord , or email (security@astaria.xyz).

If your messages contain sensitive information, you may encrypt using our PGP key:

```
Copy curl https://astaria.xyz/publickey.asc | gpg --import gpg --output document.gpg --encrypt --recipient security@astaria.xyz document
```

You may verify the authenticity of thesecurity.txt file using the following commands:

```
Copy curl https://astaria.xyz/publickey.asc | gpg --import curl https://astaria.xyz/.well-known/security.txt gpg --verify security.txt gpg: Signature made Thu Sep 21 23:31:22 2023 EDT gpg: using RSA key 0DA3BCC19A7E3197657425BDEFFB32CB832E56AD gpg: issuer "security@astaria.xyz" gpg: Good signature from "Astaria security@astaria.xyz" [ultimate]
```

Thank you for helping us keep Astaria safe!

Updated: 2024-01-24

Previous Glossary Next Audits Last updated18 days ago On this page