

Vulnerability Disclosure Policy

Version: 1.0

Issued on: 28 November 2025

Introduction

Huntsman Security (Huntsman) is a cyber security software development company providing data-driven risk management, analysis and reporting technology.

This Vulnerability Disclosure Policy (Policy) applies to any vulnerabilities you are considering reporting to Huntsman. We recommend reading this Policy fully before you report a vulnerability, and always act in compliance with it.

We value those who take the time and effort to report security vulnerabilities according to this Policy. However, we do not offer monetary rewards for vulnerability disclosures.

Reporting

If you believe you have found a security vulnerability either in our proprietary software or the Huntsman website, please submit your report to us using the following email address:

security@huntsmansecurity.com

In your report, please include the following Vulnerability Details:

- Asset (web address, IP Address, page or product name) where the vulnerability can be observed
- Title of vulnerability
- Description of vulnerability (this should include a summary, supporting files and possible mitigations or recommendations)
- Impact (what could an attacker do?)
- Steps to reproduce. These should be a benign, non-destructive, proof of concept. This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports, or malicious exploitation of some vulnerabilities.

Optional Contact Details:

- Name
- Email Address.

What to expect

After you have submitted your report, we will respond within 5 working days and aim to triage your report within 10 working days. Depending on the type of vulnerability, we may also keep you informed of our progress.

Priority for remediation is assessed by looking at the impact, severity and exploit complexity.

Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation.

We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately.

Once your vulnerability has been resolved, if it relates to our proprietary software, we will produce a Release Note and provide it directly to our customers only. **There will be no public release.** Given the nature of our software and the discrete list of users, there is no benefit to be gained by publicising your report or the Release Notes. To the contrary, it could create a further security risk for our customers. We ask you to please respect this position.

Guidance

You must NOT:

- Break any applicable law or regulations
- Access unnecessary, excessive or significant amounts of data
- Modify data in Huntsman's systems or services
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities
- Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests
- Disrupt Huntsman's services or systems
- **Access or use Huntsman's proprietary software without a valid licence**

Changes

This document will be reviewed regularly and will be updated if required.