Traceforce

Vulnerability Disclosure Policy

Version 1.0 | Effective: 2026/03/06 | Contact: cve-report@traceforce.ai

Policy Scope	Vulnerabilities discovered by Traceforce in third-party products and services
CVE Authority	Submissions routed via MITRE (cveform.mitre.org) or affected vendor CNA
Disclosure Timeline	90-day standard; 7 days for actively exploited critical issues
Primary Contact	infosec@traceforce.ai
Safe Harbor	Good-faith researchers protected per terms in Section 6

1. Introduction

Traceforce performs security research to improve the security of software and systems used by organizations and individuals worldwide. When we discover vulnerabilities in third-party products, we follow a responsible disclosure process designed to protect affected users while ensuring vendors have adequate time to remediate.

This policy describes how we handle vulnerabilities we discover, how we communicate with affected vendors, and when and how we publish our findings. It also explains how third-party researchers can report vulnerabilities to us if they relate to our own tools or infrastructure.

2. Scope

2.1 Outbound — Vulnerabilities We Discover

This policy applies to security vulnerabilities discovered by Traceforce researchers in third-party products, services, or systems. This includes:

- Model Context Protocol (MCP) servers
- Software applications (commercial, open-source, or proprietary)
- Web applications and APIs
- Cloud services and SaaS platforms

Findings are subject to this policy regardless of how the vulnerability was discovered (client engagement, independent research, bug bounty, or otherwise), unless a separate written agreement with a client specifies different terms.

2.2 Inbound — Vulnerabilities Reported to Us

We also accept vulnerability reports relating to Traceforce's own infrastructure, tools, or published software. See Section 7 for how to report to us.

3. Disclosure Timeline

We follow a 90-day coordinated disclosure timeline from the date of initial vendor notification. This timeline is aligned with industry norms established by major research organizations and gives vendors a reasonable window to develop and release patches.

3.1 Standard Timeline

Day 0	Initial notification sent to vendor via official security contact or PSIRT
Day 7	If no response, second notification sent and CVE ID requested from vendor CNA, MITRE, or CERT/CC
Day 30	Status check; timeline extension considered if vendor demonstrates active remediation
Day 90	Public disclosure regardless of patch status, unless an extension has been agreed

3.2 Accelerated Disclosure

We reserve the right to shorten the disclosure timeline to 7 days in either of the following circumstances:

- The vulnerability is being actively exploited in the wild prior to our disclosure
- Proof-of-concept exploit code has been independently published by a third party

We will make reasonable efforts to notify the vendor before accelerated disclosure, but user safety takes precedence.

3.3 Timeline Extensions

We may grant a single extension of up to 30 additional days (to a maximum of 120 days total) if the vendor: (a) acknowledges the report within 7 days; (b) provides evidence of active remediation work; and (c) communicates a credible patch release date. Extensions beyond 120 days are not granted under any circumstances.

4. CVE Assignment Process

We request CVE identifiers for all qualifying vulnerabilities we disclose. Our process depends on whether the affected vendor is a CVE Numbering Authority (CNA).

- If the vendor is a CNA, we report directly to them and they assign the CVE ID as part of the coordinated disclosure process.
- If the vendor is not a CNA, we submit a CVE request to MITRE via cveform.mitre.org at or after Day 7 if the vendor has not responded, or earlier if the vendor requests it.

- If a coordinator CNA (e.g., CERT/CC) is better placed to assist with a particular disclosure, we may route through them instead.

We include the CVE ID in all public advisories and coordinate publication timing with MITRE or the vendor CNA wherever possible.

5. Public Advisory Standards

When we publish security advisories, they will include:

- CVE identifier and CVSS score (where calculable)
- Affected product name, vendor, and version range
- Vulnerability description (type, attack vector, impact)
- Proof-of-concept or reproduction steps (at our discretion, based on risk)
- Remediation guidance or patch reference
- Credit to any collaborating researchers, unless anonymity is requested

We will not include exploit code that provides direct, weaponized attack capability in public advisories without careful consideration of the risk to users. Details may be withheld if they would primarily serve to enable attacks rather than support patching.

6. Safe Harbor

We are committed to not pursuing legal action against security researchers who report vulnerabilities to us in good faith. We consider good-faith research to include activities that:

- Do not access, modify, or exfiltrate data beyond what is necessary to demonstrate the vulnerability
- Do not disrupt production services or degrade performance for other users
- Do not target systems belonging to individuals without their consent
- Are reported to us promptly and do not involve prior disclosure to third parties

We cannot bind third parties (i.e., the vendors whose products contain vulnerabilities we research). Researchers working on third-party systems should familiarize themselves with those vendors' own safe harbor or bug bounty terms.

7. Reporting Vulnerabilities to Us

If you have discovered a security vulnerability in Traceforce’s own infrastructure, tools, or published software, please contact us at:

`cve-report@traceforce.ai`

Please include in your report:

- A description of the vulnerability and its potential impact
- Steps to reproduce or a proof-of-concept
- Any CVE or advisory references if the issue relates to a known vulnerability class

- Your preferred contact method and whether you wish to be credited

We will acknowledge receipt within 2 business days and aim to provide a substantive response within 10 business days. We follow the same 90-day timeline for disclosures reported to us, counting from the date we acknowledge the report.

8. Researcher Credit

We believe in acknowledging the work of researchers who help improve security. Unless you request anonymity, we will credit you by name in any advisory relating to a vulnerability you reported to us. For vulnerabilities we discover and report to vendors, we encourage vendors to credit Traceforce in their advisories, but we do not require it.

9. Policy Updates

This policy is reviewed at least annually and updated as our research practice evolves or as CVE program requirements change. The version number and effective date at the top of this document reflect the current revision. Material changes will be noted in our changelog below.

Version	Date	Changes
1.0	2026/03/06	Initial release

Questions about this policy? Contact us at infosec@traceforce.ai