Security Incident Response Statement

Elevatic

1 October, 2026

Table of Contents

1. Scope 3
2. Policy 4
What we consider an incident 4
How incidents and vulnerabilities reach us 4
Triage and classification 4
Remediation timeframes 4
Response process 5
Customer communication 5
3. Contact 6
4. Change history 7

1. Scope

This statement describes how Elevatic Software GmbH ("Elevatic") detects, responds to, and communicates about information security incidents and vulnerabilities affecting its Atlassian Marketplace apps. It is a summary for customers and prospects, not a substitute for our internal policies or any contractual security terms. This document is accurate as of its last published date and is reviewed annually.

2. Policy

What we consider an incident

We treat as a security incident any confirmed or suspected event that compromises the confidentiality, integrity, or availability of our apps, infrastructure, or customer data — including vulnerabilities reported by customers, researchers, or Atlassian, and anomalies surfaced by our own monitoring.

How incidents and vulnerabilities reach us

- Atlassian Marketplace Security reports
- Our regular customer support channel
- Coordinated disclosure via Atlassian's Bugcrowd program
- Automated vulnerability and dependency scanning across our codebases and infrastructure

To report a suspected security issue directly, contact security@elevatic.com.

Triage and classification

Every report is triaged for reproducibility and impact. Vulnerabilities are scored using CVSS (or the Bugcrowd Vulnerability Rating Taxonomy where applicable), which determines both the severity assigned and the remediation timeframe committed to below.

Remediation timeframes

Once a vulnerability is confirmed, Elevatic resolves it within the following timeframes, measured from the point of report or triage:

Severity	CVSS score	Timeframe for resolution
P1 – Critical	≥ 9.0	1 week
P2 – High	≥ 7.0	2 weeks
P3 – Medium	≥ 4.0	6 weeks
P4 – Low	< 4.0	20 weeks

Response process

Our response follows the industry-standard incident lifecycle:

- **Detection & triage** – the report or alert is logged, reproduced, and classified.
- **Containment** – immediate steps are taken to limit exposure while the issue is analyzed.
- **Eradication & remediation** – the root cause is fixed and a corrected release is shipped within the timeframe above.
- **Recovery** – affected systems return to normal operation under increased monitoring.
- **Lessons learned** – every incident is reviewed internally to improve our controls and processes.

Customer communication

Service availability incidents are communicated through our public status page. Security-relevant incidents — including any actual or suspected unauthorized access to end-user data, compromise of an app, or material impact to Atlassian's systems — are reported to Atlassian in line with the Atlassian Marketplace App Security Incident Management Guidelines[1]: notification within 24 hours of discovery, with status updates at least every 6 hours until the incident is resolved. Where applicable law (including the GDPR) or a contract requires us to notify affected customers or supervisory authorities directly, we do so in line with those obligations.

1. https://developer.atlassian.com/platform/marketplace/app-security-incident-management-guidelines/

3. Contact

To report a suspected security issue, contact security@elevatic.com. For general questions about this statement, contact support@elevatic.com.

4. Change history

Version	Date	Changes
1.0	01 Oct 2026	Initial draft, for review