

ZITADEL

Vulnerability Disclosure Policy

Last Updated: June 2026

Vulnerability Disclosure Policy

At Zitadel, we are deeply grateful to security researchers, ethical hackers, and community members who help protect our users and open-source ecosystems. Our goal is to collaborate transparently to identify, validate, and remediate security vulnerabilities.

To ensure our security team can focus on verified, high-impact threats and protect our customers' production environments, we require all participants to follow the rules of engagement outlined below. By reporting security issues to Zitadel, you agree to comply with this policy.

1. Safe Harbor (Authorization)

If you make a good-faith effort to comply with this policy during your security research:

- Zitadel, Inc. will consider your research to be authorized.
- We will not take legal action or terminate your access to our services.
- We will work with you to understand and resolve the issue quickly.

You must stop testing immediately and contact us if you accidentally encounter, modify, or destroy data belonging to other users.

2. Rules of Engagement & Testing Constraints

While conducting security research, the following activities are strictly prohibited:

- Any activity that violates applicable local, federal, or international laws.
- Accessing, downloading, or attempting to access or download data that does not belong to you.
- Modifying, deleting, or corrupting any data that does not belong to you.
- Executing Denial of Service (DoS, DDoS) attacks or carrying out heavy load testing.
- Engaging in physical security attacks, social engineering, phishing, or spamming Zitadel employees, clients, or users.

3. Scope

This policy applies to all systems, software, and services operated or maintained by Zitadel, including:

- **Zitadel Cloud (SaaS Platform)**: *.zitadel.cloud
- **Zitadel Websites**: zitadel.com, *.zitadel.com
- **Open-Source Software:** Codebases housed under our official GitHub organization (e.g., github.com/zitadel), in accordance with our repository security policies.

If you are unsure whether a specific asset is in scope, please contact us at security@zitadel.com before executing any testing.

4. Submission & Quality Requirements

To maintain a high standard of triage, every report must meet the following baseline requirements. Reports that fail to meet these criteria will be closed immediately without investigation.

A. Mandatory Proof of Concept (PoC)

You must provide a clear, step-by-step reproduction guide, a functional script, or a safe video demonstration of the exploit.

Zero-Tolerance for PoC Absence: Reports submitted without a reproducible, functional PoC will be marked as Invalid and closed immediately. We will not do basic discovery work on behalf of an incomplete submission.

B. Out-of-Scope Issues

We do not accept reports concerning common practices or informational listings that do not present a direct security risk. The following issues are explicitly out of scope:

- Suggestive settings regarding SPF, DKIM, DMARC, or DNSSEC.
- Missing security headers (e.g., CSP, HSTS, X-Frame-Options) unless accompanied by a PoC demonstrating a severe, actionable exploit.
- Version disclosure, server signature headers, or descriptive error messages that do not expose sensitive credentials.
- Rate limiting or brute force reports on non-critical endpoints unless they lead directly to a system-wide denial of service.
- Vulnerabilities requiring social engineering or highly improbable user actions (eg, gaining possession of an access token, compromised device, etc.).

C. Third-Party Dependencies

Zitadel actively monitors and continuously assesses all third-party dependencies using automated scanning, code analysis, and internal security auditing.

Contextual Exploitability Required: Simply running a scanner and submitting a report because Zitadel uses an outdated library or contains a known CVE is out of scope.

Requirement: To report a dependency issue, you must provide a functional PoC proving that the vulnerability is actively exploitable within the runtime context of Zitadel's specific implementation.

D. Safeguards Against AI-Generated Reports

We recognize that generative AI and LLMs can assist in research. However, we have experienced a high volume of low-quality, generic, and "hallucinated" reports.

Human-in-the-Loop Required: All reports must be verified by a human. Verbatim or raw AI-generated output (e.g., copy-pasted ChatGPT text) submitted without original, manual analysis will be rejected immediately.

Anti-Spam Measures: Submitting a high volume of unverified, AI-generated reports or automated bulk findings may result in a permanent ban of your email address, IP block, and/or reporting profile.

Silent Closure for AI Duplicates: If an AI-assisted report is identified as a duplicate of a known issue or is determined to be out of scope, Zitadel reserves the right to close the ticket without feedback.

6. Response and Resolution SLAs

We prioritize reports based on risk to our production systems and obligations to our commercial clients.

We operate under a tiered Service Level Agreement (SLA):

Tier 1: Guaranteed SLAs

We guarantee an initial response within 48 hours (2 business days) and committed engineering prioritization for reports that meet either of the following conditions:

- Commercial Clients: The report is submitted by an active, paying Zitadel client (please specify your organization name and commercial domain in the report).
- Proven SaaS Impact: The report includes a functional PoC clearly demonstrating direct, critical- or high-severity impact on the active Zitadel SaaS (Cloud) infrastructure.

Tier 2: Best-Effort Basis

For all other reports—including community findings on open-source repositories that do not directly impact our hosted SaaS environment, or non-critical issues:

We aim to acknowledge valid community reports as soon as possible.

We do not guarantee a fixed resolution SLA for community-reported bugs, open-source-only issues, or non-impactful dependencies. These are scheduled and resolved at the discretion of our product engineering team.

7. How to Report a Vulnerability

Please submit all security disclosures exclusively through our Vulnerability Disclosure Form.

Disclosures transmitted via security@zitadel.com or alternative mailboxes fall outside our tiered SLA and policy protections, and are subject to immediate rejection. Should our primary intake form be inaccessible, you may utilize security@zitadel.com while explicitly citing the system downtime. Commercial clients are further advised to initiate a concurrent support ticket through official channels.

8. Resolution, Disclosure, and CVEs

Once a report is validated:

1. Investigation: Our security team will confirm the impact and audit related code paths for similar issues.

2. Mitigation: We will build and test patches for our active releases.
3. Disclosure: Once the fix is safely applied, we will issue a CVE and publish a coordinated Security Advisory.
4. Timeline: Depending on the complexity, resolution and public disclosure can range from 7 to 90 days, according to our Policies.

9. Compensation / Bug Bounty

Zitadel does not operate a public, cash-based bug bounty program at this time.

If your report is validated, we are happy to credit you in our Security Advisory release.

For exceptionally high-impact discoveries that have saved Zitadel significant operational risk, we may offer discretionary compensation or time-and-material coverage. This requires prior, explicit written approval from Zitadel.