VULNERABILITY DISCLOSURE POLICY

ASTERISK PRIVATE BETA
JULY 2024
VERSION 1.0

Asterisk
v0.1.1

asterisk

1. Purpose

The primary objective of this Vulnerability Disclosure Policy (the "Policy") is to ensure the timely identification, verification, and resolution of security vulnerabilities in our clients' codebases. At Asterisk, we believe in responsible disclosure and collaborative efforts to enhance the overall security posture of our clients and the broader community.

2. Scope

This Policy applies to all vulnerabilities discovered by Asterisk's AI-augmented security audit system in client codebases. It outlines the processes for initial contact, vulnerability verification, and public disclosure.

3. Vulnerability Disclosure Process

3.1 Initial Contact

Upon discovery of a potential vulnerability, Asterisk will:

1. Attempt to establish communication with the client's designated security contact within 24 hours of discovery.
2. Provide a brief overview of the potential vulnerability, without disclosing sensitive details.
3. Share a link to this Policy.

If we do not receive a response within 48 hours, we will make a second attempt. If there is no response after 72 hours, we will escalate to an alternative contact provided during the onboarding process.

3.2 Vulnerability Verification

Once contact is established:

1. We will provide the client with access to our dashboard, which contains detailed information about the potential vulnerability.
2. The client will have 7 days to verify the vulnerability and provide feedback.
3. If the vulnerability is confirmed, we will work with the client to establish a remediation timeline.

3.3 Remediation and Patching

Asterisk is committed to supporting our clients throughout the remediation process:

1. We will provide detailed recommendations for addressing the vulnerability.
2. Our AI system can generate patch suggestions, which the client can review and implement.
3. We will be available for consultation throughout the remediation process.

3.4 Public Disclosure

Asterisk follows a responsible disclosure timeline:

1. We allow a standard 90-day period from the initial notification for the client to address the vulnerability.
2. If a patch is released before the 90-day period, we may disclose the vulnerability details 30 days after the patch release.
3. In cases of critical vulnerabilities or active exploitation, we may work with the client to expedite the disclosure process.

4. Confidentiality

Asterisk treats all vulnerability information as confidential until public disclosure is agreed upon with the client. We do not share vulnerability details with third parties without explicit client consent.

5. Legal Safe Harbor

Asterisk operates under the principle of good faith. We expect our clients to refrain from taking legal action against us for our security research and vulnerability disclosure efforts, provided we act in accordance with this Policy.

6. Contact Information

For any questions or concerns regarding this Policy or to report a vulnerability, please contact our security team at security@asterisk.so.

Asterisk reserves the right to modify this Policy at any time. The most current version will always be available on our website.