Otonomo’s Bug Bounty Program

5/23/2021

Johnny Jonathan, CISO and Cyber Executive

Table of Content

Contents

1 Purpose and Scope

This policy is to outline to independent security researchers, the responsible manner in which work should be carried out, while searching for vulnerabilities within the company’s infrastructure. It is important that all attacks follow the below guidelines to ensure that no legal action is taken, for lack of compliance.

These guidelines are in place, to help cyber security professionals notify the necessary parties of any vulnerabilities, or other concerns, in a responsible and time sensitive manner.

This bug bounty program is public rather than private, so no invitation or participation requests are necessary prior to submitting a report.

2 Bounty Eligibility

In order to receive the bounty for your work, you must:

- Agree to the Program Rules set out in this document.
- Remain available to supply any additional information, that may be needed to reproduce and/or remediate the issue.
- Be the first to report the particular vulnerability that you are claiming bounty for.

3 Program Rules

- Do not disclose any discovered vulnerabilities to others until the issue has been resolved.
- Do not use vulnerability scanners or other automated tools.
- Do not view, modify, damage, or delete any data belonging to others.
- Do not attempt to access other user’s accounts.
- Do not attempt any non-technical attacks. (Social engineering, phishing etc.)
- Do not degrade the experience of the service for other users intentionally.

4 Rewards

A monetary reward may be awarded to you, if:

- You are the first person to submit a site or product vulnerability.
- That vulnerability is determined to be a valid security issue by the company's security team.
- You have complied with all terms outlined in this policy.

All vulnerabilities which have been confirmed will be assessed and allocated a bounty. This bounty will be decided upon based on the vulnerability's severity. This conclusion will be reached by the company's in-house security team in its sole discretion and is final.

Every vulnerability submitted will be judged individually, and subsequent rewards shall be determined solely by the Company by several factors, namely, business impact (if not remediated), severity of the vulnerability, cost to mitigate the issue, and timeframe of submission.

There is no guarantee that a reward will be paid.

These factors are secondary to your compliance with the Bounty Eligibility and Program Rules.

4.1 Reward Categorization

Only vulnerabilities that demonstrate security impact to the system's integrity or confidentiality are eligible for a bounty. While we encourage you to submit all potential issues, lower severity issues are not eligible for bounty.

Impacts of the vulnerability submitted shall be categorized on the following criteria:

Severity (CVSS)	Risk
Critical (9.0-10.0)	Demonstrate that remote exploitation of this bug can be easily, actively, and reliably achieved.
High (7.0-8.9)	Demonstrate that remote exploitation of this bug is very likely.
Medium (4.0-6.9)	Demonstrate the presence of a security bug with probable remote exploitation potential.

Common Bounty’s

Critical	$500 +
High	$200
Medium	$100

For any bounty that is critical, the payout will start at $500 and be reviewed depending on its severity.

5 Submissions

All submissions should contain the following information, to aid in issue remediation as soon as possible.

- A clear, and detailed description of the vulnerability.
- Evidence of the vulnerability (logs, screenshots).
- Detailed steps of how to reproduce the issue.
- A personal assessment of the risk involved with the vulnerability (exploitability, potential business impacts).
- Any relevant IP addresses or URL’s.
- Any relevant platforms, operating systems, or versions.
- Full contact details

Please retain copies of any information or evidence sent in case it is needed for review.

Submissions which include the following will not be actioned.

- Denial-of-Service attacks.
- Generic vulnerability reports - supported by no evidence or relevance to our infrastructure.
- Information already in the public domain.
- Vague information
- Non-actionable issues

If you have submitted a report, which is compliant with the submission rules, we will respond as soon as possible, or once the reported issue or vulnerability has been verified.

6 Safe Harbor

Any attacks or activities which are conducted in accordance with the guidelines outlined in this policy, are to be considered as authorized conduct. No legal action will be carried out against you unless a breach of any of these rules has been committed.

If any third party is to initiate any legal action against you for actions which are authorized by this document, we will take steps to ensure that the third party is made aware of the good faith and compliance of your actions.

7 Confidentiality

Any information you receive, collect, become aware of, or comes into your possession regarding systems, staff, or customers through the bug bounty program (“Confidential Information”) must be kept confidential and only used in connection with this bug bounty program. You may not use, disclose or distribute any such Confidential Information, including, but not limited to, any information regarding your submission and information you obtain when researching the sites, without our prior written consent.