Responsible Disclosure Policy

Purpose

The purpose of Shuttlerock's Responsible Disclosure Policy is to encourage skilled security researchers to identify and report potential vulnerabilities in a safe and responsible manner. By collaborating with the security community, this policy aims to protect Shuttlerock's technology and services from exploitation, ensuring timely resolution of any identified weaknesses while safeguarding user data and privacy.

Scope

The scope of this Responsible Disclosure Policy is strictly limited to vulnerabilities identified within Shuttlerock's Cloud system and does not apply to any other systems, services, or infrastructure outside of this environment.

The scope of this policy includes all security researchers, ethical hackers, and individuals who report vulnerabilities related to Shuttlerock's Cloud system. It also applies to Shuttlerock employees, contractors, and any third-party vendors who are responsible for managing or securing the Shuttlerock Cloud system.

Roles and Responsibilities

Security Researcher:

- Responsible for identifying and reporting potential vulnerabilities in compliance with the Responsible Disclosure Policy.
- Should refrain from exploiting the vulnerability and must allow Shuttlerock reasonable time to address the issue before making it public.
- Expected to maintain confidentiality regarding the vulnerability until it has been resolved.

IT Director:

- Oversee the overall implementation and enforcement of the Responsible Disclosure Policy, ensuring alignment with Shuttlerock's security strategy.
- Review and approve vulnerability resolution timelines, ensuring critical issues are addressed promptly.
- Approve the payment for any rewards to bug reporters, based on the severity and impact of the vulnerability.

Developers:

- Analyze the reported vulnerabilities and work closely with the IT team to resolve them efficiently.
- Develop and test patches or updates to address the identified vulnerabilities, ensuring that the fix is effective without introducing new risks.

- Assess the potential vulnerability and provide an indication of value in terms of a financial reward (if any) to be paid to the Bug Reporter.

Systems Administrators:

- Acknowledge the receipt of vulnerability reports within the designated timeframe and maintain communication with the bug reporter throughout the investigation.
- Collaborate with security teams and Developers to verify, prioritize, and address reported vulnerabilities.

Guidelines for Reporters

In our Responsible Disclosure Policy, we encourage ethical behavior from security researchers and community members who wish to help us enhance our systems' security. Adhering to these guidelines will enable us to address vulnerabilities effectively and securely while safeguarding our users and data.

Expectations for Ethical Behavior

- We expect all reporters to act in good faith and with integrity. Please approach your research responsibly, with the goal of helping us identify and address security issues, not exploiting or publicizing them in ways that could harm the organization or our users.
- Respect the privacy and confidentiality of our users, their data, and our systems. Do not access, modify, or delete any data beyond what is strictly necessary to demonstrate a potential vulnerability.

Avoid Actions that Could Cause Harm

Data Integrity

- Avoid any actions that could result in data deletion, modification, or corruption. Please refrain from testing vulnerabilities on live data or user accounts.

Service Continuity

- Do not engage in any activity that might cause disruption to our services, systems, or users. This includes actions that could overload or impair our network, such as denial-of-service (DoS) attacks.

User Privacy

- Do not use vulnerabilities to access or disclose personal information. Our priority is to protect our users' data and ensure their privacy is maintained.

Provide a Detailed Vulnerability Report

To help us understand and address the issue, we ask that you provide a comprehensive report. Please include:

Description of the Vulnerability

- Clearly describe the nature of the issue, including what type of vulnerability it is (e.g., XSS, SQL injection).

Steps to Reproduce

- Outline the exact steps we should follow to replicate the issue. This will help us verify and understand the root cause quickly.

Impact Assessment

- Describe the potential impact of the vulnerability on our systems, data, or users, including how it could be exploited.

Proof of Concept (PoC)

- If possible, provide screenshots, code snippets, or any other evidence that demonstrates the vulnerability in action without compromising user data.

By following these guidelines, you can help us resolve issues efficiently, maintain system integrity, and protect user data throughout the responsible disclosure process.

Safe Harbor & Legal Protection

Our organization is committed to creating a collaborative environment where security researchers can responsibly disclose vulnerabilities without fear of legal repercussions. We value the contributions of researchers and will take measures to protect those who act in good faith and abide by our Responsible Disclosure Policy.

Assurances Against Legal Action

- If you act in accordance with our Responsible Disclosure Policy and operate in good faith to report vulnerabilities, we assure you that we will not initiate legal action against you. This protection applies to those who:
    - Follow the guidelines set forth in this policy
    - Avoid accessing or compromising any user data beyond what is necessary to demonstrate the vulnerability
    - Cease testing and notify us promptly upon identifying a potential issue
- We will work closely with researchers who comply with these guidelines and operate within legal boundaries to address any vulnerabilities in our systems.

Good-Faith Activities and Intentions

- Our organization considers activities conducted in good faith under this policy to be authorized, and we will treat your research as legitimate and welcomed. Good-faith activities include:
    - Actions aimed solely at identifying and responsibly reporting vulnerabilities, without intent to exploit or cause harm

    - Compliance with our guidelines to minimize impact on our systems and users
    - Respecting user privacy and refraining from accessing unnecessary data
- We encourage all researchers to approach their work with integrity and transparency. If you have any questions regarding whether your planned actions align with our policy, please reach out to us for clarification before proceeding.

How to Report a Vulnerability

- If you believe you've identified a security vulnerability, please fill out an official form at the following URL. https://shuttlerock.atlassian.net/servicedesk/customer/portal/2/create/100. A member of our team will acknowledge your report within four (4) weeks.
- When submitting a vulnerability report, researchers are encouraged to include detailed information such as steps to reproduce the issue, proof of concept, screenshots, logs, and any other relevant data to help streamline the investigation and resolution process.

Assessment Process

We are committed to collaborating with you to address any reported vulnerabilities effectively and transparently. Here's what you can expect from our process:

Acknowledgment and Initial Response

- Upon receiving your report, we will acknowledge receipt within 48 hours. Our initial response will confirm that we have received your submission and may include a preliminary assessment or request for additional details if necessary.

Triage Process and Communication

- Our security team will review and assess the reported vulnerability to determine its impact and severity. During this triage process, we may reach out for further clarification or additional information.
- We will keep you informed of significant updates at key stages in the process, including once we have verified the vulnerability and as we work towards a resolution and possible bug bounty. You can expect regular communication from our team throughout.

Expected Resolution and Fix Timelines

- We aim to resolve verified vulnerabilities as quickly as possible, based on their severity and impact on our systems. Critical issues may be addressed immediately, while lower-severity issues might take longer to fix.
- We will do our best to provide you with an estimated timeline for resolution once the triage process is complete. After a fix is deployed, we may follow up with you for verification.

Rewards and Payments

Shuttlerock may offer discretionary rewards to security researchers who report valuable vulnerabilities in accordance with this Responsible Disclosure Policy. The amount of the reward will be determined based on the severity, impact, and complexity of the vulnerability. Rewards are not guaranteed and are issued solely at the discretion of the IT Director.

To be eligible for a reward, bug reporters must provide accurate contact details, including any necessary banking information, if requested. Failure to provide accurate details may result in delays or forfeiture of the reward. All decisions regarding the eligibility and amount of the reward are final and cannot be appealed.

Shuttlerock reserves the right to withhold rewards if the vulnerability is already known or if it does not meet the criteria outlined in this policy.

Exclusions

While researching, we'd like you to refrain from the following activities:

- Distributed Denial of Service (DDoS) attacks
- Automated vulnerability scanning that may disrupt services
- Testing or accessing out-of-scope systems
- Accessing, modifying, or deleting confidential data
- Exploiting vulnerabilities beyond proving their existence
- Spamming
- Social engineering or phishing of Shuttlerock employees or contractors
- Any attacks against Shuttlerock's physical property or data centers

Non-Compliance or Misuse

We are committed to working with security researchers in a respectful and collaborative manner. However, actions taken outside the scope of this Responsible Disclosure Policy may result in the loss of safe harbor protections and potential legal consequences.

Consequences for Non-Compliance

- If a reporter fails to adhere to the guidelines outlined in this policy, including those related to ethical behavior, responsible reporting, and respect for user data, we reserve the right to take appropriate action. This may include revoking safe harbor protections and, in severe cases, involving law enforcement or taking legal action.

Unacceptable Actions

Extortion or Threats

- Any attempt to demand payment or threaten exposure of a vulnerability before our team has had an opportunity to address the issue will be treated as extortion and may lead to legal consequences.

Data Tampering or Deletion

- Modifying, deleting, or corrupting data as part of vulnerability research is strictly prohibited and may lead to immediate revocation of safe harbor protections.

Service Disruption

- Activities that disrupt or degrade our services, such as denial-of-service attacks, are not permitted and may result in legal action.

Unauthorized Disclosure

- Publicly disclosing any details of a vulnerability without our explicit consent is unacceptable and may jeopardize the security of our systems and users.

Security Contact

Shuttlerock is always open to feedback, questions, and suggestions. If you would like to talk to us, please feel free to email us at security@shuttlerock.com.

Responsibility

It is the IT Directors responsibility to see this policy is enforced.

Last updated: November 2024