afero®
4410 El Camino Real
Suite 200
Los Altos, CA 94022
USA

Vulnerability Disclosure Policy

Last Updated 2024-03-18

Table of Contents

Introduction

Afero takes its responsibility to protect customer data very seriously. This Vulnerability Disclosure Policy (“Policy”) provides guidance to third-party Security Researchers who identify security vulnerabilities in Afero-powered products and services and wish to report the same to Afero.

Definitions

Afero-powered products and services: Firmware for devices, applications for mobile platforms, cloud-hosted services, and IT infrastructure that is written, programmed, developed, or used by Afero for our customers.

Customer: An Afero customer is an entity that owns an ecosystem and sells Afero-powered products and services, it is not the end user that may purchase a product or device from one of our customers.

Security Researcher. A computer professional who identifies and analyzes vulnerabilities in hardware, software, firmware, applications, and cloud services and may use various techniques to discover and exploit security flaws. Afero employees are not eligible Security Researchers under this Policy and should submit security vulnerabilities directly to the Security Team.

Security Vulnerability: A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, can result in a negative impact to the confidentiality, integrity, or availability of Afero data or systems.

Exceptions

This Policy confers no rights or entitlements of any kind, whether financial, in law or in equity, or otherwise, on any Security Researcher or other person or entity. All aspects of this policy and process are subject to change without notice and on a case-by case basis. No particular level of response is guaranteed for any specific issue or class of issues.

Product Security Incident Response Team

The Afero Product Security Incident Response Team (PSIRT) is responsible for responding to reports submitted pursuant to this Policy. Specifically, the PSIRT manages the receipt, investigation, and response to reports about security vulnerabilities and issues related to Afero-powered products and services.

Policy

This Policy applies to all vulnerabilities in Afero-powered products and services that are reported to Afero.

Afero values those who take the time and effort to report security vulnerabilities according to this policy, however, this Policy does not offer monetary rewards or any other compensation for vulnerability disclosures.

By submitting a vulnerability, the Security Researcher acknowledges there is no expectation of payment and expressly waives any future pay claims against Afero related to the submission.

This Policy covers how Afero addresses reported security vulnerabilities in Afero-powered products and services, including timelines, actions, and responsibilities.

Afero may change this Policy at any time by posting the revised Policy at the location defined in the secruity.txt file. Security Researchers are responsible for reviewing the Policy and ensuring compliance with any changes made. Security Researchers participating in any research after changes become effective will be subject to the revised Policy.

Bug Bounty Program

Afero does not currently offer a Bug Bounty program.

Authorization

Security research performed within the scope of and in compliance with this Policy is authorized by Afero, and Afero will not recommend, refer, or pursue legal action against the Security Researcher related to the research and/or report. Should legal action be initiated against the Security Researcher by a third party for activities conducted in accordance with this Policy, Afero will make its authorization known to the party initiating the legal action, the court, etc.

Reporting a Vulnerability

If you believe you have found a security vulnerability in Afero-powered products and services that has not been resolved, please contact Afero PSIRT at the following email address.

psirt@afero.io.

Requests to this email address are normally read and acknowledged with a non-automated response within three business days.

Afero welcomes reports from independent security researchers, industry organizations, vendors, customers, and other sources concerned with product or network security.

To help protect our customers, we request that Security Researchers do not post or share any information about a potential vulnerability in any public setting until Afero has researched, responded to, and addressed the reported vulnerability, and if needed, informed our customers.

What to Send

When submitting a vulnerability or security related issue to Afero PSIRT, please provide as much information about the issue as possible. This includes but is not limited to:

1. Information about the related product or service (product name, version number, service name, website, IP or page where the vulnerability can be observed.)

2. A detailed description of the vulnerability and its type (e.g., "XSS vulnerability"), including the location where the vulnerability was discovered and the potential impact of exploitation.
3. Date the vulnerability was observed.
4. Steps to reproduce or instructions on how to duplicate the vulnerability. These can be written steps, a video, or a set of screen captures detailing a benign and non-destructive proof of concept.
5. Your name and company (if applicable). Reports may be submitted anonymously.
6. Your preferred contact information (email, phone, etc.).
7. Your PGP or GPG public key to allow for encrypted communication (if available).
8. Reports **MUST** be submitted in English.

This information will help expedite verification of the vulnerability and ensure that the report can be triaged quickly and accurately.

Afero will not claim ownership rights to submissions pursuant to this Policy. However, by providing any submission to Afero, the Security Researcher grants Afero a worldwide, perpetual, royalty-free, irrevocable, nonexclusive, fully sublicensable (through multiple levels) license to use, reproduce, modify, adapt, create derivative works, translate, publish, publicly perform, publicly display, broadcast, transmit, distribute, and otherwise exploit the contents of any submission for any purpose and in any form, medium, or technology now known or later developed. The content of any submissions will not be treated as proprietary or confidential to the Security Researcher.

Sensitive Information and Data Markings

Afero PSIRT honors Traffic Light Protocol (TLPv2) (https://www.first.org/tlp/) data markings.

All non-public information shared with Afero PSIRT about security issues will be kept confidential within Afero, except to the extent that a disclosure is required legally, under contract, pursuant to a subpoena or court order, or necessary to protect Afero's rights or property. Similarly, Afero PSIRT asks Security Researchers to maintain strict confidentiality until complete resolutions are available.

Vulnerability information anonymized to protect its source may be shared with Afero customers and partners if necessary to protect the privacy and security of them and their businesses.

Afero PSIRT may work with and share information with third-party coordination centers such as the Computer Emergency Response Team Coordination Center (CERT/CC) and the Cybersecurity and Infrastructure Security Agency (cisa.gov), to be handled under their coordinated vulnerability disclosure process. Afero will not share the Security Researcher's contact information without express prior permission, unless otherwise required by law or court order.

Afero will protect customer-specific data at all times throughout this process. Specifically, Afero will not share any customer-specific data unless directed to do so by the affected customer, or as required by law or necessary for its investigation.

Secure Communication

Afero encourages Security Researchers to encrypt sensitive information that is sent by email. Afero PSIRT and Afero Security supports encrypted messages via Pretty Good Privacy (PGP)/GNU Privacy Guard (GPG) encryption software and uses an OpenPGP key to secure email communications.

The following key is used for communicating securely with Afero and email sent to psirt@afero.io or security@afero.io may be encrypted with the following public key. This key may also be used to verify the signature of any Afero published security advisories. (This key may change from time to time, so check this part of the Policy for updated keys.)

Afero's Public Key: Download Key

Afero PSIRT Key ID as of 2024-01: **3BD43C9E45C621C1**

Fingerprint: **F624 21E2 E353 B7D9 8816 F547 3BD4 3C9E 45C6 21C1**

Please do not send messages encrypted with this public key to any address other than psirt@afero.io or security@afero.io as we are unable to accept any non–security-related email which is encrypted with this public key.

Concerns

If you feel your security concern was not dealt with in a satisfactory manner, please contact the Afero Security Team at the following email address.

security@afero.io

Response Process

Afero PSIRT will work with internal teams to verify the findings, triage the report, assign prioritization, and may request additional information if needed.

Priority for remediation is assessed by looking at the impact, severity and exploit complexity.

Afero PSIRT will notify the reporter when the reported vulnerability is remediated, and invite them to confirm that the solution covers the vulnerability adequately.

The steps in the process are as follows:

1. **Awareness:** PSIRT receives notification of a security incident.
2. **Active Management:** PSIRT prioritizes and identifies resources.
3. **Software Fixes:** PSIRT coordinates the fix and performs an impact assessment.

Afero PSIRT investigates all reports regardless of the Afero software code version or product life cycle status until the product reaches the Last Day of Support (LDoS). Issues will be prioritized based on the potential severity of the vulnerability and other factors.

With the agreement of the Security Researcher, Afero PSIRT may acknowledge the reporter's contribution during any public disclosure of the vulnerability.

Communications Plan

Once Afero PSIRT has verified and validated a vulnerability or incident it may notify customers, if necessary.

Guidance & Legalities

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give Security Researchers permission to act in any manner that is inconsistent with the law, or which might cause Afero or partner organizations to be in breach of any legal obligations. When assessing a vulnerability in Afero-powered products and services one **MUST NOT**:

- Violate any applicable laws or regulations.
- Access any customer data or data relating to any identifiable person.
- Modify data in the organization's systems or services.
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities.
- Attempt any form of denial of service (DoS or DdoS) attack (i.e., overwhelming a service with a high volume of requests or other network traffic.)
- Disrupt the organization's services or systems.
- Submit reports detailing non-exploitable vulnerabilities.
- Communicate any vulnerabilities or associated details other than by means described in this Policy.
- Social engineer or ‘phish’ Afero employees, contractors, or personnel.
- Undertake any physical testing of Afero’s buildings or infrastructure (e.g., office access, open doors, tailgating).
- Demand financial compensation in order to disclose any vulnerabilities.
- Violate the privacy of the organization's users, staff, contractors, services, or systems for example, by sharing, redistributing, or failing to properly secure data retrieved from the systems or services.
- Make use of any discovered vulnerability after confirming its existence.

One **MUST**:

- Always comply with data protection rules.

- Securely delete all data retrieved during your research as soon as it is no longer required or within 1 month of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).
- Provide Afero with a reasonable amount of time to resolve the issue before public disclosure.

Assessing Security Risk

Afero uses CVSS version 4.0 to score vulnerabilities and takes into consideration several factors such as active exploitation, customer exposure, and public disclosure timelines while prioritizing response actions for issues.

Severity	Remediation	Customer Notification
Actively exploited or high exploit potential	Patched ASAP.	Within 48 hours of verification and validation
Critical CVSS > 9	Designated as a blocker for the next scheduled maintenance release.	Within 72 hours of verification and validation
High CVSS >=7	Designated as a high priority for the next release.	Documented in monthly customer briefings or advisories
Medium CVSS >=4	Designated as a medium priority for the next release.	Documented in release notes
Low CVSS < 4 and not mitigated by BCPs	May be fixed in the next major version.	Documented in release note
Low CVSS < 4 and mitigated by BCPs	May be fixed in the next major version.	Documented in release notes

There can be exceptional issues which cannot be sufficiently fixed or mitigated in a reasonable timeline. Such issues may require actions by standardization organizations, or depend on an upstream organization to deliver fixes, or require inventing a new hardware architecture. In such cases, Afero PSIRT may publish an advisory with possible mitigations and workarounds, but no remediations involving a product change.

Cloud-Hosted Services

Afero runs multiple cloud-hosted services that are used by customers but are maintained, patched, and monitored by Afero.

Afero PSIRT responds to vulnerabilities in Afero cloud-hosted services and works closely with the teams that operate them. These teams ensure that security vulnerabilities are fixed and patches are deployed to all customer instances in a timely manner.

Typically, service-related security events are communicated to customers by the service teams through direct notification or through the service dashboard or portal. In some instances, Afero may disclose vulnerabilities through security advisories.

In most cases, no user action is required because Afero regularly patches cloud-hosted services.

Third-Party Software Vulnerabilities

If there is a vulnerability in a third-party software component that is used in Afero-powered products and services, Afero will typically use the CVSS score provided by the component creator. However, Afero may adjust the CVSS score up or down to reflect the impact to Afero-powered products and services.

Afero may determine a third-party vulnerability to be “high” based on consideration of the following:

- Number of Afero-powered products and services that may be affected.
- A CVSS score of 5.0 or above.
- The vulnerability has gathered significant public attention.
- The vulnerability is likely to have exploits available and is expected to be, or is being, actively exploited.

For high profile third-party vulnerabilities that are a real threat, Afero will begin assessing all potentially impacted Afero-powered products and services that have not reached the LDoS.

Security Software Updates

Afero PSIRT will investigate and disclose vulnerabilities in Afero-powered products and services from the date of First Commercial Shipment (FCS) to the LDoS.

After End of Sale (EoS), the availability of security fixes for vulnerabilities is defined in the product’s EoS bulletin. The EoS bulletin may define the Last Day of Support (LDoS) milestone, which identifies the last date that Afero will investigate and disclose product vulnerabilities.

Once the LDoS has been reached, Afero PSIRT will continue to accept vulnerability reports but will not analyze, fix, or disclose potential vulnerabilities. To this end, Afero PSIRT will not issue CVEs for issues reported on products that are past the LDoS milestone.

Non Emergency and General Security-Related Queries

For general nonsensitive and non-emergency security concerns regarding Afero-powered products and services, please contact the Afero Security Team at the following email address.

security@afero.io

Public Relations or Press Security-Related Queries

Public relations or press queries regarding Afero security vulnerability information should be sent to the following email address.

press@afero.io

Commitment to Product Security and Integrity

Afero product development practices specifically prohibit any intentional behaviors or product features that are designed to allow unauthorized device or network access, exposure of sensitive device information, or a bypass of security features or restrictions. These include, but are not limited to:

- Undisclosed device access methods or "back doors"
- Hardcoded or undocumented account credentials
- Covert communication channels
- Undocumented traffic diversion

Afero considers such product behaviors to be serious vulnerabilities. Afero PSIRT will address any issues of this nature with the highest priority and encourage all parties to report suspected vulnerabilities to Afero PSIRT for immediate investigation. Internal and external reports of these vulnerabilities will be managed and disclosed in accordance with the terms of this Policy.

Security.txt

Afero supports an RFC 9116-compliant security.txt file, located at

https://www.afero.io/.well-known/security.txt