ubicquia®

Vulnerability Disclosure Policy

Last Modified: April 26, 2024

This Vulnerability Disclosure Policy is part of Ubicquia, Inc. (“**Ubicquia**” or the “**Company**”) commitment to the security of its customers and the wider internet community. Ubicquia values the contributions of security researchers and users who take the time and effort to report security vulnerabilities according to this policy. Ubicquia will act in good faith to resolve reported vulnerabilities in accordance with this policy.

1**. Introduction**

This document outlines the vulnerability disclosure policy for Ubicquia. This policy aims to ensure the security and integrity of the Company’s products and services while fostering collaboration with the security research community. Ubicquia is committed to the responsible handling of vulnerabilities in accordance with this policy. This policy applies to any vulnerabilities that are being considered to report the Company and we recommend reading this policy before you report a vulnerability.

2. **Reporting Vulnerabilities**

Security researchers or users who discover vulnerabilities in the Company’s products or systems are encouraged to report them via email: vulnerability@ubicquia.com.

In the report, please provide the details below:

* The website, IP or page where the vulnerability can be observed.

* A brief description of the type of vulnerability, for example; “XSS vulnerability”.

* Steps to reproduce. These should be a benign, non-destructive, proof of concept. This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports, or malicious exploitation of some vulnerabilities, such as sub-domain takeovers.

3. **Commitments**

The Company commits to acting on disclosed vulnerabilities in a timely manner. Upon receiving a report, we will evaluate the issue and take necessary steps to address it.

The Company will exercise commercially reasonable effort to acknowledge receipt of vulnerability reports within 5 working days and to triage such report within 10 working days. Any written acknowledgment by the Company will include an initial assessment of the report and next steps.

Priority for remediation is assessed by looking at the impact, severity and exploit complexity. We prioritize the handling of critical vulnerabilities to ensure they are addressed with appropriate urgency.

Ubicquia will provide regular status updates pursuant to existing contractual obligations. At a minimum, the Company will be providing status updates at least every two weeks until the issue is resolved.

4. **Resolution Process**

Investigation and Validation: Upon receipt of a vulnerability report, Ubicquia's security team will conduct an initial investigation to validate the issue.

Remediation: The Company will develop a remediation plan to address the vulnerability. This may include temporary workarounds, patches, or updates to our products or systems.

6. **Guidance**

You must **NOT**:

- Break any applicable law or regulations.
- Retrieve, access, modify any data in the Company's systems or services.
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities.
- Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests.
- Disrupt the Company's services or systems.
- Submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with "best practice", for example missing security headers.
- Submit reports detailing TLS configuration weaknesses, for example "weak" cipher suite support or the presence of TLS1.0 support.
- Communicate any vulnerabilities or associated details other than by means described in the contact details.
- Social engineer, 'phish' the Organization.
- Demand financial compensation in order to disclose any vulnerabilities.

You must:

- Always comply with data protection rules and must not violate the privacy of the Organization's users, staff, contractors, services or systems. You must not, for example, retrieve any data from our systems.

- Should someone mistakenly retrieve data from our systems, all data retrieved must be securely deleted immediately upon realization (this data must not be shared, redistributed).

6. **Contact**

For further information or to submit a vulnerability report, please contact us via email: vulnerability@ubicquia.com. This contact method is secured to protect the confidentiality of the information shared.

7. **Legalities**

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, code of ethics, or which might cause the Company or partner organizations to be in breach of any legal obligations.