Responsible Disclosure policy

1.0, 2024-08-01: Printed

Table of Contents

Copyright . . . 1
Revision History . . . 2
1. Introduction . . . 3
2. Why participate? . . . 4
3. Rules of engagement . . . 5
    3.1. Safe harbour for researchers is applied . . . 5
4. Scope . . . 6
5. Application . . . 7
6. Scoring . . . 9
7. Bounties . . . 10
8. Exclusions . . . 11
9. Feedback . . . 12

Copyright

Revision History

Revision	Date	Comments
1.0	2024-08-01	Printed

Chapter 1. Introduction

Responsible Disclosure indicates Magnolia's continued commitment to improve its security posture. As part of this process, we work closely with security researchers to identify and report vulnerabilities they find within our systems. Magnolia appreciates security researchers efforts in reporting vulnerabilities on its systems as long as the discovered vulnerability is in scope, detected without the use of intrusive testing techniques, and follows the disclosure guidelines below.

At Magnolia, the safety of internet presence and the continuity of our online services are our top priorities. Our specialists work continuously to optimize our systems and processes. Despite the effort we put into the security of our systems, vulnerabilities can still be present.

Example 1. 📢 Call for ethical hackers

> Do you have the skills and have you discovered any vulnerabilities in our systems? Please help by reporting them to us, so that we can improve the safety and reliability of our systems together.

Chapter 2. Why participate?

To encourage reporting vulnerabilities to Magnolia, we would urge you to send any vulnerability you detect to us. Any researcher who provides a high quality report which will be important for the continuity and reliability of the bank might be invited to the **private security testing program** where financial reward(s) are possible after the invitation.

We’ve done our best to clean up our known issues and now would like to request your help to spot the ones we missed.

Chapter 3. Rules of engagement

1. Reports are required to be written in English. Please include a clear attack scenario outlining detailed reproduction steps.
2. Make sure that during your investigation you do not cause any damage or disruptions to our systems so do not alter, change or delete data from our systems. Do not put a backdoor in the system, not even for the purpose of showing the vulnerability as inserting a backdoor will cause even more damage to the safety of our systems and do not penetrate the system any further than required for the purpose of your investigation.
3. Make sure that during your research you do not inadvertently cause a data breach (e.g., sharing screenshots or recordings on a 3rd-party cloud solutions).
4. Law regulations for Responsible Disclosure may differ by country.

We strongly advise you to take these regulations into account. Your investigation on our systems could be regarded as a criminal act under local or international law and you may then risk criminal prosecution. If you have detected vulnerabilities in one of Magnolia's systems, please be aware that local law takes precedence over Magnolia rules.

Nevertheless, if you act in good faith and according to Magnolia's rules, we will not report your actions to the authorities, unless required to do so by law.

3.1. Safe harbour for researchers is applied

Magnolia considers ethical hacking activities conducted consistent with the Researcher Guidelines, the Program description and restrictions (the Terms) to constitute "authorized" conduct under criminal law. Magnolia will not pursue civil action or initiate a complaint for accidental, good faith violations, nor will they file a complaint for circumventing technological measures used by us to protect the scope as part of your ethical hacking activities.

If legal action is initiated by a third party against you and you have complied with the Terms, Magnolia will take steps to make it known that your actions were conducted in compliance and with our approval.

Chapter 4. Scope

In scope:

- Any Magnolia owned domains and subdomains.

Out of scope:

- Domains not owned by Magnolia.

Chapter 5. Application

- Pre-Auth Account takeover/OAuth squatting
- Self-XSS that can’t be used to exploit other users
- Verbose messages/files/directory listings without disclosing any sensitive information
- CORS misconfiguration on non-sensitive endpoints
- Missing cookie flags
- Missing security headers
- Cross-site Request Forgery with no or low impact
- Presence of autocomplete attribute on web forms
- Reverse tabnabbing
- Bypassing rate-limits or the non-existence of rate-limits.
- Best practices violations (password complexity, expiration, re-use, etc.)
- Clickjacking on pages with no sensitive actions
- CSV Injection
- Sessions not being invalidated (logout, enabling 2FA, etc.)
- Mixed content type issues
- Cross-domain referrer (referrer header) leakage
- Anything related to email spoofing, SPF, DMARC or DKIM
- Content injection on error pages
- Username/email enumeration
- Email bombing
- HTTP Request smuggling without any proven impact
- Homography/typosquatting
- XMLRPC enabled
- Banner grabbing/Version disclosure
- Open ports without an accompanying proof-of-concept demonstrating vulnerability
- Weak SSL configurations and SSL/TLS scan reports
- Not stripping metadata of images
- Disclosing API keys without proven impact
- Same-site scripting
- Blind SSRF without proven impact (DNS pingback only is not sufficient)
- Disclosed and/or misconfigured Google API key (including maps)
- Host header injection without proven impact
- Spam, social engineering and physical attacks

- DOS/DDOS attacks or brute force attacks
- Reports that state that software is out of date/vulnerable without a proof-of-concept
- Attacks requiring physical access to a victim's computer/device, man in the middle or compromised user accounts

Chapter 6. Scoring

We use the CVSS v4.0 Standard Common Vulnerability Scoring system

Chapter 7. Bounties

This is a responsible disclosure program **without bounties**.

Furthermore, this program is not intended for reporting:

- Complaints about Magnolia's services or products
- Questions about the availability of Magnolia websites or services

Chapter 8. Exclusions

- In case that a reported vulnerability was already known to the company from their own tests or other reporting, it will be flagged as a duplicate.
- Theoretical security issues with no realistic exploit scenario(s) or attack surfaces, or issues that would require complex end user interactions to be exploited, may be excluded or be lowered in severity.
- Vulnerabilities that are limited to non-current browsers (older than 3 versions or two years) will not be accepted.
- Do not utilize social engineering in order to gain access to our systems.

Vulnerabilities detected by Magnolia employees or former employees of Magnolia are welcomed but excluded from any rewards.

Chapter 9. Feedback

Would you like to help us improve our program or have some feedback to share, please send your anonymous feedback to disclosure-program@magnolia-cms.com

Feedback is checked periodically and must not be used for submission or support queries.