Responsible Disclosure Policy

Document status

Owner	Security Officer
Classification	PUBLIC
Status	APPROVED
Approved on	01 Apr 2020

Policy

Introduction

Security is core to our values, and we value the input of researchers acting in good-faith to help us maintain a high standard for the security and privacy for our users. This includes encouraging responsible vulnerability research and disclosure. This policy sets out our definition of good-faith in the context of finding and reporting vulnerabilities, as well as what you can expect from us in return.

Expectations

When working with us according to this policy, you can expect us to:

- Work with you to understand and validate your report, including a timely initial response to the submission; we strive to acknowledge receipt within 1 day and verify the issue within 48 hours;
- Work to remediate discovered vulnerabilities in a timely manner; and
- Recognize your contribution to improving our security if you are the first to report a unique vulnerability, and your report triggers a code or configuration change.

Scope

- *.greenmini.nl
- *.greenmini.host
- *.greenminihost.com
- Systems hosted within our network AS205668, which are owned and operated by Green Mini host

If you are in doubt, please feel free to contact us at: security@greenmini.nl

Out-of-Scope

- All systems, websites, servers, etc. owned and operated by *customers* of Green Mini host
- Services hosted by 3rd party providers

If you are in doubt, please feel free to contact us at: security@greenmini.nl

In the interest of the safety of our users, staff, the Internet at large and you as a security researcher, the following test types are excluded from scope:

- Findings from physical testing such as office access (e.g. open doors, tailgating)
- Findings derived primarily from social engineering (e.g. phishing, vishing)
- UI and UX bugs and spelling mistakes
- Network level Denial of Service (DoS/DDoS) vulnerabilities

Rewards

If you want, we will publicly thank you and acknowledge your efforts in our Hall of Fame or other communication platforms. We will only give a monetary compensation in very exceptional cases, but please do not ask for it.

You will be free to publicise the found vulnerabilities, but we request to give us at least 90 days to resolve the issue, and keep the vulnerability confidential in the mean time

Disclosure Policy

Ground Rules

To encourage vulnerability research and to avoid any confusion between legitimate research and malicious attack, we ask that you attempt, in good faith, to:

- Play by the rules. This includes following this policy any other relevant agreements;
- Report any vulnerability you've discovered promptly;
- Avoid violating the privacy of others, disrupting our systems, destroying data, and/or harming user experience;
- Use only the communication channels listed in this policy to discuss vulnerability information with us;
- Handle the confidentiality of details of any discovered vulnerabilities according to our Disclosure Policy;
- Perform testing only on in-scope systems, and respect systems and activities which are out-of-scope;
- If a vulnerability provides unintended access to data: Limit the amount of data you access to the minimum required for effectively demonstrating a Proof of Concept; and cease testing and submit a report immediately if you encounter any user data during testing, such as Personally Identifiable Information (PII), Personal Healthcare Information (PHI), credit card data, or proprietary information;
- You should only interact with test accounts you own or with explicit permission from the account holder; and
- Do not engage in extortion.

Safe Harbor

When conducting vulnerability research according to this policy, we consider this research conducted under this policy to be:

- Authorized in view of any applicable anti-hacking laws, and we will not initiate or support legal action against you for accidental, good faith violations of this policy;
- Authorized in view of relevant anti-circumvention laws, and we will not bring a claim against you for circumvention of technology controls;
- Exempt from restrictions in our Acceptable Usage Policy that would interfere with conducting security research, and we waive those restrictions on a limited basis; and
- Lawful, helpful to the overall security of the Internet, and conducted in good faith.

You are expected, as always, to comply with all applicable laws. If legal action is initiated by a third party against you and you have complied with this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please submit a report through one of our communication channels before going any further.

How to report

If you believe you've found a security vulnerability in one of our products or platforms please send it to us by emailing security@greenmini.nl. Please include the following details with your report:

- Description of the location and potential impact of the vulnerability;
- A detailed description of the steps required to reproduce the vulnerability (POC scripts, screenshots, and screen captures are all helpful to us); and
- Your name/handle and a link for recognition in our Hall of Fame.

If you'd like to encrypt the information, please use our paste server https://tmp.greenmini.host and send us the password via telephone: +31208932333 or Wire: @gmh_soc / security@greenmini.nl

This policy is based on disclose.io and bugcrowd