certero.

Vulnerability Disclosure Policy

Version: 1

May 2023

Public

Revision History

Version	Version Date	Comments / Amendments
1a-d	May – December 2022	Initial draft versions
1e	April – May 2023	Revisions made
1	24th May 2023	Moved to final

Document Information

Status:	Final
Author:	Sarah Knowles
Owner:	Chief Information Security Officer
Approved By:	Chief Information Security Officer / Operations Director
Next Planned Review Date:	May 2024

Document Rights

This document remains the exclusive property of Certero. Any offer made in this document is subject to agreement on terms and conditions unless there is an explicit statement to the contrary within this document. Should there be any errors or omissions contained within this document, Certero reserves the right to adjust any details accordingly and post an updated version on the Certero website.

Location and Contact Details

Up to date contact, location and company registration details can be found via our website:

http://www.certero.com

Trademark Acknowledgements

Acquaintia, AssetStudio, Certero App-Centre, Certero Acquaintia Reporting Made Easy, certero for certain for sure, Passworks, PowerStudio, and Vitado are the registered trademarks of Certero Ltd in the UK and in other jurisdictions worldwide. All other trademarks belong to their respective holders registered in many jurisdictions worldwide.

Table of Contents

1. About this document

1.1. Introduction

This disclosure document should be read in full before reporting any vulnerabilities. This helps to ensure that the policy is understood and complied with.

Certero actively endorse and support working with the research and security practitioner community to improve our online security.

We are committed to:

- investigating and resolving security issues in our platform and services thoroughly
- working in collaboration with the security community
- responding promptly and actively

1.2. Scope

This disclosure policy applies only to vulnerabilities in Certero products and services under the following conditions:

- 'In scope' vulnerabilities must be original, previously unreported, and not already discovered by internal procedures.
- Volumetric vulnerabilities are not in scope - meaning that simply overwhelming a service with a high volume of requests is not in scope.
- Reports of non-exploitable vulnerabilities, or reports indicating that our services do not fully align with "best practice", for example missing security headers, are not in scope.
- TLS configuration weaknesses, for example "weak" cipher suite support or the presence of TLS1.0 support, are not in scope.
- The policy applies to everyone, including for example Certero staff, third party suppliers and general users of the Certero public services.

2. Bug Bounty

Certero do not offer a paid bug bounty programme. However we will make efforts to show appreciation to security researchers who take the time and effort to investigate and report security vulnerabilities according to this policy where possible.

3. Reporting a Vulnerability

If you have discovered something you believe to be an in-scope security vulnerability, first you should check the above details for more information about scope, then submit a vulnerability report via email to disclosures@certero.com

In your submission, include details of:

- The location, i.e. website or page where the vulnerability can be observed.
- A brief description of the type of vulnerability, for example an 'XSS vulnerability'.

Your report should provide a benign, non-destructive, proof of exploitation wherever possible. 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 subdomain takeovers.

3.1. What to Expect

After submitting your vulnerability report, you will receive an acknowledgement reply usually within 72 working hours of your report being received.

The team will triage the reported vulnerability, and respond as soon as possible to let you know whether further information is required, whether the vulnerability is in or out of scope, or is a duplicate report. If remediation work is necessary, it is assigned to the appropriate Certero team for resolution.

Priority for bug fixes or mitigations is assessed by looking at the impact severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status of the process, but should avoid doing so more than once every 14 days. The reason is to allow our teams to focus on the reports as much as possible.

When the reported vulnerability is resolved, or remediation work is scheduled, the Vulnerability Disclosure Team will notify you, and invite you to confirm that the solution covers the vulnerability adequately.

4. Guidance

Security researchers must NOT:

- Access unnecessary amounts of data. For example, 2 or 3 records is enough to demonstrate most vulnerabilities, such as an enumeration or direct object reference vulnerability.
- Use high-intensity invasive or destructive technical security scanning tools to find vulnerabilities.
- Violate the privacy of Certero users, staff, contractors, services or systems. For example, by sharing, redistributing and/or not properly securing data retrieved from our systems or services.
- Communicate any vulnerabilities or associated details using methods not described in this policy.
- Modify data in the Certero systems or services.
- Disrupt Certero services or systems.
- Social engineer, 'phish' or physically attack Certero staff or infrastructure.
- Disclose any vulnerabilities in Certero systems or services to 3rd parties or the public, prior to Certero confirming that those vulnerabilities have been mitigated or rectified. However, this is not intended to stop you notifying a vulnerability to 3rd parties for whom the vulnerability is directly relevant. An example would be where the vulnerability being reported is in a 3rd party software library or framework. Details of the specific vulnerability as it applies to Certero must not be referenced in such reports.
- Require financial compensation in order to disclose any vulnerabilities outside of a declared bug bounty reward structure (such as holding an organisation to ransom).

We ask you to delete securely any and 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.

5. 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, or which might cause Certero to be in breach of any of its legal obligations, including but not limited to:

- The Computer Misuse Act (1990)
- The General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018
- The Copyright, Designs and Patents Act (1988)
- Privacy and Electronic Communications Regulations

Please ensure that you fully comply with the data protection regulations and laws applicable to your region with regards to any relevant information that is contained within this document. Certero affirms that it will not seek prosecution of any security researcher who reports any security vulnerability on a Certero service or system, where the researcher has acted in good faith and in accordance with this disclosure policy. This is not a license or invitation to reverse engineer our Intellectual Property which would still initiate legal action.