CBUAE Classification: Public

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

VULNERABILITY DISCLOSURE POLICY

Vulnerability Disclosure Policy

Document information	
Policy Title:	Vulnerability Disclosure Policy

Revision history				
Version Number	Release Date	Summary of Changes	Sections	Changes Made By
0.1	29-July-2021	Initial version	N/A	Information Security Team
0.2	7-February-2022	Final version	N/A	Information Security Division

TABLE OF CONTENTS

INTRODUCTION

The Central Bank of the UAE ("CBUAE") takes responsibility for data protection in maintaining the security of its financial systems. This vulnerability disclosure policy aims to provide transparent guidelines to researchers to enable them to discover security protection vulnerabilities, and to provide a clear overview of how the identified vulnerabilities should be submitted to us.

This policy presents a description of the covered research types and systems, a procedure for submitting vulnerability reports to us, and the terms of vulnerability proceedings, including the waiting period for the security researchers prior to public disclosure of the reported vulnerabilities.

We welcome and encourage your reports to us to ensure the disclosure and removal of potential system vulnerabilities.

1 AUTHORISATION

Provided that you adhere to this policy's provisions in the course of your security research, we will guarantee our co-operation with you to gain an insight into the issues, and to resolve them as soon as possible. In such cases, your research will be viewed as authorised, and the CBUAE will neither pursue nor recommend initiating legal action pertaining to the conducted research. If a third party initiates legal action against you related to security research activities compliant with our policy, we will declare your authorised status.

2 GUIDELINES

In the framework of this policy, the term "research" covers activities that satisfy the following conditions:

- You have provided us with immediate notification on discovery of any security issue, or potential issue;
- You have made every effort to prevent violation of your privacy, data manipulation, destruction of the information, deterioration of the user experience, and production system destabilisation;
- You have worked only in the context required for the confirmation of the available vulnerability issue. Exploits should not be used for any data exfiltration or compromise, pivoting to a different system, or setting persistent access to the command line;
- You have allowed us to offer a resolution within a reasonable timeframe, prior to public disclosure of the vulnerability issue;
- You have submitted a report of adequate quality and length. Please allow us a reasonable amount of time to resolve the issue before you disclose it publicly; and
- You do not submit a high volume of low-quality reports.

On identifying an available vulnerability, or the presence of such sensitive data as financial details, personal details, trade secrets, or proprietary data of any party, we expect you to notify us immediately, without any further disclosure of the identified issue or continuation of the test.

3 TESTING METHODS

We do not authorise the following methods of testing:

- Non-technical testing, in particular social engineering (such as vishing, phishing, etc.), physical testing (such as tailgating, opened doors, office access, etc.):
- Vulnerability testing of third-party websites, services, or applications linked from or to CBUAE systems, or integrated with them:
- DoS or DDoS tests, or any other network denial of service tests that cause damage to the related data or systems, and interrupt access to them:
- Testing systems different from those mentioned in the section 'Scope' below;
- Testing which can either cause intentional disruption, disability, or impairment of CBUAE systems, or lead to the degradation of the CBUAE system's functioning;
- Testing that allows the introduction of malicious software;
- Retaining, sharing, altering, or deleting CBUAE data;
- Denying access to CBUAE data; or,
- Testing with the use of exploits aimed at data exfiltration, pivoting to a different CBUAE system, establishing access to the command line, or maintaining a constant presence on CBUAE systems.

4 SCOPE

Application of this policy is limited to the following services and systems:

- *.centralbank.ae, *.cbuae.gov.ae,

Only the services on the list above have our corresponding authorisation for testing, and are included in the permitted scope. This does not cover any vulnerabilities identified in our vendors' systems; in such cases, a corresponding report is to be sent to the relevant vendor in strict accordance with their vulnerability disclosure policy, if any.

We request active testing and research only in the scope of services and systems covered in this policy, regardless of whether we are engaged in the development and maintenance of other internet-based services and systems. We encourage you to present your concerns for further discussion on any systems outside the aforementioned scope that you believe require testing.

5 REPORTING A VULNERABILITY

The only purpose of reports submitted under this vulnerability disclosure policy is to ensure the protection of the data as well as remediation or mitigation of all available vulnerabilities. Should your research findings cover any previously unknown vulnerabilities that affect the CBUAE or its service or product users, we will consider sharing them with government cybersecurity agencies, trade associations, CERTs or other entities to initiate an official process of vulnerability disclosure, according to their policy. We will disclose your contact details or name only if you have given your corresponding consent.

You may submit your reports anonymously. We accept them via either information.security@cbuae.gov.ae or the online vulnerability report form.

You will receive confirmation of the report's receipt within three business days of sharing your contact details with us.

5.1 What We Expect From You

Proper processing and prioritising of the provided reports requires your adherence to the conditions below:

- A detailed description of the vulnerability's location, and the possible effect of its use;
- Please provide screenshots and concept script proofs with a detailed presentation of the measures required for vulnerability reproduction; and
- We prefer reports to be completed in the English language, if possible.

5.2 What You May Expect from Us

If you share your contact information with us, we guarantee transparent communication without any delays:

- We send acknowledgements of report receipts within three business days;
- We provide corresponding confirmation of the vulnerability, to the best of our ability. We ensure maximum transparency of measures taken in the course of any remediation process, with the potential challenges and issues related to the issue resolution covered.
- We guarantee open communication to discuss all vulnerability issues.

6 QUESTIONS

We will answer questions sent to information.security@cbuae.gov.ae on this policy, and will take your comments and suggestions on possible responses.