digiteal

REINVENTING INVOICING AND PAYMENT

Coordinated Vulnerability Disclosure Policy

Introduction

In computer security, coordinated vulnerability disclosure, or "CVD" (formerly known as responsible disclosure) is a vulnerability disclosure model in which a vulnerability or an issue is disclosed to the public only after the responsible parties have been allowed sufficient time to patch or remedy the vulnerability or issue.
Coordinated Vulnerability Disclosure is a form of disclosure: the transfer of information from an external source to a company or organization, in this case regarding the security of IT systems.
There are four ways a researcher or criminal can handle the information of a vulnerability:

1. **Non-disclosure** : the researcher or criminal keeps the information to themselves. Often because they either fear legal repercussions when sending in or to use the vulnerability as leverage.

2. **Limited Disclosure** : the researcher or criminal shares only a limited amount of information to a limited number of parties. This puts pressure on companies to quickly fix the vulnerability to prevent exploitation.

3. **Full Disclosure** : the researcher or criminal releases the vulnerability publicly. This puts companies at risk if they cannot resolve the issue fast enough.

4. **Coordinated Vulnerability Disclosure** : the researcher directly contacts the company with a report that isn't shared publicly until the vulnerability is fixed.

Full disclosure: Why it's not ideal

Occasionally a security researcher may discover a flaw in our app. This leaves the researcher responsible for reporting the vulnerability. In most cases, an ethical hacker will privately report the breach to our team and allow our team a reasonable timeframe to fix the issue. In some cases, **they may publicize the exploit to directly alert the public**.

Disclosing a vulnerability to the public is known as full disclosure, and there are different reasons why a security researcher may go about this path.

- A security researcher may disclose a vulnerability if:
- They are unable to get in contact with the company.
- Their vulnerability report was ignored (no reply or unhelpful response).
- Their vulnerability report was not fixed.
- They felt notifying the public would prompt a fix.
- They are afraid of legal prosecution.

While not a common occurrence, full disclosure can put pressure on our development team and PR department, especially if the hacker hasn't first informed our company. These scenarios can lead to negative press and a scramble to fix the vulnerability.

Digiteal considers it important that its information and systems are secure.

Digiteal is committed to ensuring the security of our clients by protecting their information from unwarranted disclosure. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

This policy describes **what systems and types of research** are covered under this policy, **how to send us** vulnerability reports, and **how long** we ask security researchers to wait before publicly disclosing vulnerabilities.

We want security researchers to feel comfortable reporting vulnerabilities they've discovered – as set out in this policy – so we can fix them and keep our users safe. We have developed this policy to reflect our values and uphold our sense of responsibility to security researchers who share their expertise with us in good faith.

Despite our concern for the security of these systems, it may occur that there still is a vulnerability.

If you have found a vulnerability in one of our systems, please let us know so that we can take measures as quickly as possible. We would like to work with you to protect our audience and our systems in a better way.

We have therefore opted for a policy of coordinated disclosure of vulnerabilities (also known as the 'Responsible Disclosure Policy') so that you can inform us when you discover a vulnerability.

This Responsible Disclosure Policy applies to all Digiteal’s systems. In any case of doubt, please contact us to clarify matters via security@digiteal.eu or on https://support.digiteal.eu.)

Responsible disclosure

At Digiteal we greatly value the support of IT security researchers and members of cybersecurity communities in helping us to maintain our high IT security standards.

If you identify an IT security vulnerability relating to any of our websites please notify us promptly before disclosing the vulnerability to the outside world, so that we can take the necessary measures. This is known as responsible disclosure.

Please keep all information relating to the discovered vulnerability secret from all third parties for a period of at least 90 days, allowing us to identify and implement the measures needed to address the issue you have reported.

What does Digiteal include in our Coordinated Vulnerability Disclosure Policy ?

Our Coordinated Vulnerability Disclosure program sets up guidelines for researchers on

- what to report vulnerabilities on and
- how we will handle them.

This program gives the researcher guidelines and a framework within which they can start their investigation. It also creates transparency about how the vulnerabilities are disclosed: the researcher directly contacts Digiteal with a report that isn’t shared publicly until the vulnerability is fixed. By having a Coordinated Vulnerability Disclosure program, we make clear what type of vulnerabilities we are looking for and what we promise to do with a report.

Scope

The current scope for reporting is defined in the Bug Bounty Program Policy.

Rules of Engagement

The rules of engagement are defined in the Bug Bounty Program Policy.

How does Digiteal manage reports coming in via a Coordinated Vulnerability Disclosure Policy ?

Handling many reports - about many vulnerabilities - can become overwhelming. A dedicated platform allows researchers to report vulnerabilities without you needing to set up additional security infrastructure.

Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorised, we will work with you to understand and resolve the issue quickly, and Digiteal will not recommend or pursue legal action related to your research.

Guidelines

Under this policy, “research” means activities in which you:

- Follow the rules of engagement.
- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability’s presence. Do not use an exploit to compromise or exfiltrate data, establish command line access and/or persistence, or use the exploit to “pivot” to other systems.

- Provide us a reasonable amount of time to resolve the issue before you disclose it publicly.
- You do not intentionally compromise the privacy or safety of Digiteal personnel (e.g. employees or collaborators), or any third parties.
- You do not intentionally compromise the intellectual property or other commercial or financial interests of any Digitealpersonnel or entities, or any third parties.

Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), **you must stop your test, notify us immediately, and not disclose this data to anyone else.**

What we ask of you

If you discover a vulnerability in one of our systems, we ask you to:

- Report the vulnerability as soon as possible after discovery. Mail your findings to security@digiteal.eu.
- Provide sufficient information to reproduce the vulnerability so that we can solve the problem as quickly as possible. Usually the IP address or URL of the affected system and a description of the vulnerability is sufficient, but for more complex vulnerabilities more may be needed.
- Leave your contact details, so that Digiteal can contact you to work together for a safe result. Leave at least your name, e-mail address and/or telephone number. Reporting under a pseudonym is possible, but make sure that we can contact you if we should have additional questions.
- Confirm that you have acted and will continue to act in accordance with this Responsible Disclosure Policy.

We also have a Bug Bounty Program Policy for reporting vulnerabilities.

What we promise

- If you have complied with the above terms of the Responsible Disclosure Policy and have not committed any other breaches, we will not take any legal action against you.
- We will respond to your report within a short period of time, if possible within 10 working days, with our review of the report and any expected date for resolution.
- We will treat your report confidentially and will not share your personal data with third parties without your consent unless this is necessary to comply with a legal obligation.
- We will keep you informed of the progress of solving the problem.
- To thank you for any report of a security problem that is not yet known to us, we offer the opportunity to be listed in our "Hall Of Fame". We strive to solve all problems within a short period of time.
- We may choose to ignore low quality reports.

If you have any questions, we encourage you to address them to security@digiteal.eu.
In case of doubt about the applicability of this policy, please contact us first via this email address, to ask for explicit permission.

We reserve the right to change the content of this Policy at any time, or to terminate the Policy.

Privacy statement

Your private data are managed securely in respect of the GDPR.

Disclosure

Digiteal is committed to timely correction of vulnerabilities. However, we recognize that public disclosure of a vulnerability in absence of a readily available corrective action likely increases versus decreases risk. Accordingly, we require that you refrain from sharing information about discovered vulnerabilities for 90 calendar days after you have received our acknowledgement of receipt of your report. If you believe others should be informed of the vulnerability prior to our implementation of corrective actions, we require that you coordinate in advance with us.

We will not share names or contact data of security researchers unless given explicit permission.

Questions

Questions regarding this policy may be sent to security@digiteal.eu. We also invite you to contact us with suggestions for improving this policy.