Vulnerability Disclosure Policy

Clark Holding SE

Version 1.0 - last updated 01.04.2024

Introduction

This Vulnerability Disclosure Policy (VDP) outlines the procedures and guidelines for the responsible disclosure of security vulnerabilities affecting the products and services of Clark Holding SE and its subsidiaries, hereinafter referred to as "the Company." This policy is designed to foster collaboration with the security community, ensuring the confidentiality, integrity, and availability of our systems and data in compliance with GDPR and other relevant European regulations. The Company recognizes the importance of transparency and cooperation in maintaining a secure environment for our customers and stakeholders.

Scope

This policy applies to all individuals, including security researchers, customers, and third-party vendors, who discover potential security vulnerabilities within the Company's products and services. The scope of this policy includes, but is not limited to, software applications, web applications, mobile applications, network infrastructure, and any other digital assets owned or operated by the Company.

Contents of this policy

Responsible Disclosure

The Company encourages individuals who discover security vulnerabilities to report them promptly in accordance with the following guidelines:

Report Submission

Vulnerabilities should be reported to the Company's designated contact point for security disclosures. Contact information for reporting vulnerabilities can be found on the Company's website (*https://www.clark.io/vulnerability-disclosure-program/*)
Reports should include detailed information about the vulnerability, including steps to reproduce, impact assessment, and any relevant supporting materials such as screenshots or proof-of-concept code.
Reporting criteria:

1. Add as many details as possible to the reports.
2. Provide screenshots of your process.
3. When possible, provide the code used as POC, it will help us reproduce and validate your report.

Cooperation

The Company is committed to acknowledging receipt of vulnerability reports within a reasonable timeframe.
Upon receiving a report, the Company will work collaboratively with the reporter to validate and address the reported vulnerability.

Confidentiality

The Company respects the confidentiality of reporters and will handle vulnerability reports with the utmost discretion.
Reporters are encouraged to provide contact information for follow-up communication, but anonymous reports will also be accepted and evaluated.
If agreed to, reporters have the possibility to share their social media handles to appear in the Company’s Hall of Fame, and contact details to receive a thank you letter.

Any data on the Company, the Company’s employees or the Company’s customers that is being transmitted through the Vulnerability Disclosure Program must be kept confidential.
Reports may only be disclosed after remediation and after receiving the Company’s written consent. Any disclosure of confidential information outside of this requirement will result in immediate legal proceedings.

Timely Resolution

The Company will make reasonable efforts to investigate and remediate reported vulnerabilities in a timely manner.
Reporters will be notified of the resolution status and any remediation actions taken by the Company.

Rewards

If after evaluation and triage, the report qualifies, the Company offers the reporter a place in the Company's hall of fame and goodies for meaningful reports. Outstanding reports may qualify for monetary rewards.

Exclusions

The following actions are expressly prohibited under this policy:

Disruptive Attack Methods

Any attempt to exploit or test vulnerabilities using disruptive attack methods are strictly forbidden, including but not limited to:

- Distributed Denial of Service (DDoS)
- Physical attacks on the properties or providers
- Social engineering (incl. Phishing, vishing, spear phishing)
- Attempts to disrupt the integrity, confidentiality or availability of the Company's data

Reporters engaging in such activities will be subject to legal action and may be reported to relevant authorities.

Unauthorised Access

Any attempt to gain unauthorised access to the Company's systems, data, or networks is prohibited and may result in legal consequences. Proof of concepts are sufficient to qualify as a vulnerability report.

Out of Scope vulnerabilities

The Company excludes from the scope of this vulnerability disclosure program:

- Any vulnerability already known to the Company
- Vulnerabilities submitted without details

- Vulnerabilities that only affect browsers which are outdated or only have limited security features
- Unused best practices in headers, SSL/TLS, DNS and insecure ciphers
- Reports generated by scanners that do not provide specific and traceable references to a vulnerability
- Missing cookies flags on non-sensitive cookies
- Vulnerabilities in 3rd party application or providers

Legal

The Company acknowledges that security researchers play a crucial role in identifying and mitigating Information Security risks. To this end, the Company commits to:

- Not pursuing legal action against individuals who discover and report vulnerabilities in good faith and in accordance with this policy.
- Providing safe harbour for vulnerability disclosure activities conducted in compliance with this policy.

The testing must not violate any law, disrupt services, or compromise any data of the Company. By participating in the program, reporters agree to comply with applicable regulations in terms of personal data protection such as GDPR and applicable European standards.

Compliance

This policy is subject to periodic review and updates to ensure alignment with evolving regulatory requirements and industry best practices. By participating in the Company's Vulnerability Disclosure Program, individuals agree to abide by the terms and conditions outlined in this policy.

For inquiries related to vulnerability disclosure, please contact disclosure@clark.io

Acknowledgment:

By submitting a vulnerability report to the Company (meaning sending an email to disclosure@clark.io), individuals acknowledge that they have read, understood, and agreed to comply with the terms and conditions of this Vulnerability Disclosure Policy.

Effective Date: 01.04.2024

This policy is effective as of 01.04.2024 and supersedes any previous versions.