Vulnerability Disclosure Policy

SUMMARY

Security and privacy are Artefaktum's primary objectives. We employ a variety of tools and processes to continually analyse and improve our security practices. However, the constant evolution of threats makes it impossible for our team to stay ahead of all potential vulnerabilities.

To help us keep ahead of emerging threats and vulnerabilities, we welcome arbitrary security research surrounding our Services. All internet-facing assets are in scope, with preference given to issues. For details contact us at any time.

We provide safe harbour for the Computer Fraud and Abuse Act ("CFAA") and the Digital Millennium Copyright Act ("DMCA"), as well as any similar or successor legislative actions for all research that is conducted in good faith. We also permit and encourage responsible disclosure of any vulnerability findings, as long as any and all such disclosures do not violate the confidentiality of any in-scope or Artefaktum customer data.

LEGAL TERMS

By participating in this policy, you agree to and are bound to the terms and conditions detailed in this page. These terms are governed by Colorado law, and constitute the entirety of the agreement between you and Artefaktum. Any changes to the terms in this policy must be made in writing and agreed upon by both parties.

Artefaktum will not publicly disclose the identity of any researcher that reports a vulnerability through this policy without their consent unless required to do so by law.

If litigation is initiated against you by a third party based on your disclosure(s) and your actions are fully in compliance with the terms and conditions of this policy, Artefaktum may, at its own and sole discretion, take reasonable steps to notify concerned parties that your actions were conducted in full compliance with our policy.

Unless Artefaktum is required by federal, state, or local law enforcement, Artefaktum does not intend to pursue legal action against research, researchers, or disclosures that are conducted in good faith, adhere to the strictest standards of confidentiality in terms of data ownership, and meet Artefaktum Terms of Service.

CONDUCTING RESEARCH AND TESTING

Automated vulnerability scanning tools are strictly prohibited, and may result in being banned from further research participation and/or legal action where applicable.

You may only conduct research and tests on publicly available resources and endpoints, or with your rightfully assigned user account. You may not attempt to gain access to any other user's account. You may not compromise or attempt to compromise any other user's account or any confidential information that is owned by Artefaktum.

All research and tests must not disrupt, intercept, or compromise any data that you do not own, or violate any international, federal, state, or local laws or regulations,

In the event of an inadvertent violation or disruption of service (e.g. you access another user's data, change any service configurations, etc.), immediately report the incident to sec_team@artefaktum.net. Any and all data that was accessed during the course of research or testing must not be recorded, stored, used, disclosed, or further accessed in any way.

DISCLOSURE REPORTING PROCEDURES

All submissions require explicit written permission from an authorised Artefaktum representative to disclose the results of a submission. Any public disclosures made without explicit written permission from Artefaktum will disqualify the reporter from all future participation under this policy, and will be prosecuted to the furthest extent of all applicable law.

If you have discovered a vulnerability, please collect and send as many of the following points as possible to mail@artefaktum.net:

- Screenshots of the UI, console, or tool dashboards throughout the collection and analysis process (no links if possible)
- Detailed steps to replicate the vulnerability
- Affected endpoint

SEE NEXT PAGE APPROVED AND DISAPPROVED SUBMISSION TYPES

ENCOURAGED SUBMISSION TYPES:

- OWASP Top 10
- Business Logic vulnerabilities
- Information Disclosure
- Data Exposure
- Authorization/authentication issues

EXCLUDED SUBMISSION TYPES:

- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Spam reports
- Phishing, vishing, spear phishing reports
- Social engineering reports
- Open ports with no accompanying demonstration or proof of concept of vulnerability
- Findings generated by automated tools without detailed explanation on what parts are vulnerable and how the vulnerability might be exploited

DISCLAIMER

This policy does not guarantee monetary rewards for submissions.

Artefaktum reserves the right to change, remove, or modify the terms and conditions of this policy at any time, with or without notice. Before sending each submission, please review the terms of this policy to ensure full compliance.

Artefaktum cannot guarantee any response or remuneration for reported vulnerabilities. However, Artefaktum will make our best effort to acknowledge receipt of the reported vulnerability and other pertinent and disclosable information to the reporter within a reasonable period of time. Factors that influence the response timeline include the severity, likelihood, and impact of the vulnerability, as well as the current obligations and priorities of the Artefaktum Security team.