Responsible Disclosure Policy

ALFAIATE - SYSTEMS, UNIPESSOAL, LDA (ALFASOFT)

Version 1.0

Our commitment

At ALFASOFT we take the security of the systems we build and maintain as seriously as we take their functioning. However carefully we develop, no software is free of flaws.

If you have found a vulnerability in an ALFASOFT system, or in a system we developed for a client, we want to hear about it. This policy sets out how to report your finding, what you can expect from us, and what we ask of you in return.

We are grateful to those who report security problems in good faith. That work helps us protect our clients and the users of their services.

How to report

Send your report to:

security@alfasoft.pt

We accept reports in Portuguese or in English.

If you would like to encrypt your report, say so in your first message and we will send you the corresponding public key.

What to include in your report

The more complete the information, the faster we can reproduce and fix the problem. Wherever possible, please tell us:

- The system, address or component affected
- The type of vulnerability and the impact you attribute to it
- The steps needed to reproduce the problem
- Supporting evidence — logs, screenshots, request or response excerpts
- The approximate date and time at which you carried out your testing
- A contact through which we can clarify questions and keep you informed of progress

A full proof of exploitation is not required. A description of the problem and of the steps to reproduce it is enough.

What you can expect from us

Stage	Our commitment
Within 3 business days	We acknowledge receipt of your report
Within 10 business days	We complete our initial assessment and tell you whether we could reproduce the problem, the severity we have assigned to it and the remediation plan foreseen
During remediation	We keep you informed of progress, with regular updates

Stage	Our commitment
After remediation	We confirm the fix and, if you so wish, publicly acknowledge your contribution

If the vulnerability affects a system we operate on behalf of a client, we inform that client as promptly as the severity of the case requires, since the decision on the remediation timeline rests with them. Your identity is not shared without your consent.

If we decide not to fix the problem — for instance, because we consider the risk residual or the mitigation already present at another level — we explain the reasoning behind that decision.

What we ask of you

So that we can handle your report under this policy, we ask that you:

- **Do not exploit the vulnerability** beyond what is strictly necessary to demonstrate that it exists
- **Do not access, alter, transfer or delete data** that is not yours. If, in the course of testing, you inadvertently access third-party data, stop testing immediately and let us know
- **Do not degrade or disrupt services**, and do not carry out denial-of-service testing, bulk messaging or automated brute-force testing
- **Do not resort to social engineering**, to the manipulation of staff or clients, or to physical access to our premises
- **Do not disclose the vulnerability publicly** before a fix is available, or before 90 days have elapsed since your report, whichever comes first. If you need a different timeline, talk to us — we will find a schedule acceptable to both parties

Safe harbour

If you meet the conditions of this policy, ALFASOFT undertakes to:

- **Not initiate or support any legal action or complaint** against you as a result of your research and report
- Treat your report as a good-faith contribution, and not as an attempted unauthorised access
- Where a third party brings action against you for acts carried out in compliance with this policy, make public that your conduct fell within it

This undertaking covers your conduct alone. It does not displace the rights of third parties nor any legal obligations to which ALFASOFT is subject.

Outside the scope of this policy

The following are not, as a rule, treated as security vulnerabilities:

- Output from automated scanning tools without a demonstration of real impact
- Absence of configuration best practices that is not exploitable — for example, missing security headers with no associated attack vector
- SPF, DKIM or DMARC configuration, without a demonstration of exploitation
- Attacks requiring physical access to the device, or an already compromised device

- Denial-of-service or resource exhaustion attacks
- Disclosure of software versions with no known associated vulnerability
- Vulnerabilities in third-party services not operated by ALFASOFT

Even so, if you believe one of these cases has concrete impact, describe it — we review every report we receive.

Rewards

ALFASOFT does not currently run a monetary bug bounty programme. We publicly acknowledge, with your consent, those who report valid vulnerabilities to us.

Contact

Vulnerability reports: security@alfasoft.pt

General enquiries: info@alfasoft.pt · +351 211 452 611

ALFAIATE - SYSTEMS, UNIPESSOAL, LDA · Rua Vasco da Gama, n.º 49, 1.º Dto., 2000-232 Santarém, Portugal

This policy is reviewed annually. Changes are published on this page, with an indication of the date on which they take effect.