

## Vulnerability Disclosure / Reporting Security Vulnerabilities / Alphatech spol. s r. o.

### Introduction

We take the security of our products seriously. If you have discovered a security vulnerability in an Alphatech product or service, please report it responsibly using the contact below. Your report helps us protect customers and improve the security of our solutions.

### Contact

Email: [security@alphatech.cz](mailto:security@alphatech.cz)

### Recommended Report Contents

To help us verify and resolve the issue quickly, please include:

- product name / model and the affected function (e.g., web UI, API, update mechanism)
- firmware / software version (and, if available, serial number or other device ID)
- environment and configuration (briefly: network setup, operating mode, open services/ports)
- description of the vulnerability and expected vs. actual behavior
- steps to reproduce (ideally step by step)
- evidence / supporting materials (logs, screenshots, Wireshark PCAP) if available
- information on whether you have any indication of active exploitation in the wild (IoCs, timestamps, source IPs, etc.)

### How We Will Proceed

- We will acknowledge receipt of your report as soon as possible, typically within 24 hours.
- The report will be logged and assigned an identifier.
- We may contact you for additional information or to verify details.
- If a significant vulnerability is confirmed, we will prepare corrective measures (mitigation / update) and, if needed, issue a security advisory.

### Coordinated Disclosure

We kindly request coordinated disclosure. Please do not publish details of the vulnerability before a fix or at least a temporary mitigation is available. If you plan to publish, please contact us in advance so we can coordinate the process.

### Security Testing

Please refrain from testing that:

- could disrupt the availability of customer services,
- involves accessing data belonging to others without consent,
- or affects devices and systems you do not own or do not have permission to test.

### Legal Framework and Communication

In the case of incidents or actively exploited vulnerabilities, we may be required to fulfill legal notification obligations to the relevant authorities. Our priority is to quickly reduce impact and inform affected customers with practical recommendations.

### Acknowledgement

Thank you for reporting responsibly. Security is a team effort — and your report helps us protect our customers.

