

ZIV

VULNERABILITY DISCLOSURE POLICY

Content

1. INTRODUCTION 3
2. PURPOSE AND PRINCIPLES 3
3. SCOPE OF APPLICATION 3
4. GUIDELINES FOR GOOD-FAITH SAFETY INVESTIGATIONS 4
5. HOW TO REPORT A VULNERABILITY 5
6. MANAGEMENT OF REPORTED VULNERABILITIES 6
7. COORDINATED DISCLOSURE, CONFIDENTIALITY AND DATA 7
8. VULNERABILITIES IN THIRD-PARTY COMPONENTS 8
9. LEGAL FRAMEWORK AND RESERVATION OF RIGHTS 8

1. INTRODUCTION

ZIV APLICACIONES Y TECNOLOGÍA, S.L.U. (hereinafter "ZIV") is firmly committed to the cybersecurity of its products and solutions. This policy sets out a framework for responsibly reporting, analysing and managing security vulnerabilities that may affect products, solutions or components supplied by ZIV.

2. PURPOSE AND PRINCIPLES

The aim of this policy is to facilitate the coordinated reporting of security vulnerabilities and to establish clear rules for investigations carried out in good faith. ZIV believes that effective vulnerability management helps to reduce risk throughout the product lifecycle and to protect the confidentiality, integrity and availability of the systems into which they are integrated.

ZIV would like to thank researchers, customers, system integrators and security professionals for the time and effort they put in to report vulnerabilities responsibly and in accordance with this policy. Unless expressly stated otherwise in a specific programme, ZIV does not offer financial rewards for this type of communication.

3. SCOPE OF APPLICATION

This policy applies to ZIV products and solutions that incorporate digital components, software or firmware, including, but not limited to:

- Protection and control equipment.
- Metering, monitoring and automation equipment.
- Communications equipment.
- Platforms, applications and software tools associated with ZIV products.
- Firmware, communication interfaces and digital services supplied as part of a ZIV solution.

Third-party systems, services or infrastructure that are neither owned nor controlled by ZIV fall outside the scope of this policy. Any vulnerabilities identified in third-party products, services or components integrated into ZIV's products or solutions that may affect their security must be reported to ZIV via the channel set out in this policy. Where a vulnerability affects only third-party products, services or components that are not integrated into ZIV's products or solutions, it is recommended that you report it directly to the relevant manufacturer or supplier.

4. GUIDELINES FOR GOOD-FAITH SAFETY INVESTIGATIONS

ZIV values and appreciates the responsible reporting of potential security vulnerabilities. This policy does not constitute a general authorization to access the systems, networks, equipment or information of ZIV, its clients or third parties. Any research must be carried out on the organization's own systems or equipment, or on systems or equipment for which the relevant authorization has been granted, whilst complying with the limits set out in this policy. It also requests that researchers and third parties refrain from carrying out tests or activities that could compromise the security, availability or integrity of its products, systems and services, affect its users or result in the loss, alteration or corruption of data.

If, during an investigation, a vulnerability is identified that allows access to sensitive information, such as personal data, financial information, confidential information or third-party trade secrets, the investigator must immediately cease testing, notify ZIV PSIRT of the finding and refrain from accessing, using, retaining or disclosing such information, except to the extent strictly necessary to document and report the vulnerability securely.

ZIV has no intention of taking legal action against those who carry out security investigations in good faith, within the limits set out in this policy and without causing harm or infringing the rights of third parties. Whilst this undertaking relates exclusively to actions falling within ZIV's remit, it does not limit the powers of the authorities or the rights of third parties. In any event, any act committed in bad faith, as well as any breach of these guidelines or of the applicable legislation, may give rise to the relevant legal liabilities.

5. HOW TO REPORT A VULNERABILITY

Anyone who identifies a potential vulnerability affecting a ZIV product or solution may report it to the ZIV Product Security Incident Response Team (ZIV PSIRT) as set out below:

Email address	product.security@zivautomation.com
PGP encryption	PGP public key Fingerprint: D613 1C19 3134 509B 65C4 2825 E246 25F3 F7D6 3483

It is recommended that the report be written in Spanish or English and, wherever possible, include:

- Details of the product or service concerned, model, firmware/software version and any reference numbers required to identify the version unequivocally.
- Technical description of the vulnerability, including probable cause, impact, preconditions, estimated severity and observed outcome.
- Reproduction steps, tools used and, where necessary, a minimal, non-destructive proof of concept. Relevant screenshots, images, videos or network traces may be attached.
- Equipment configuration, test environment topology and a list of other connected components, where this information is required to analyze the case.
- Contact details, where the notifier wishes to provide them, to enable the notification to be tracked and to facilitate coordination in the event of a release. Anonymous submissions will be accepted.

The absence of any of these elements will not prevent the reporting of a potential vulnerability. ZIV may request further information where this is necessary for its analysis.

To protect the information exchanged, ZIV recommends maintaining the highest possible level of confidentiality throughout the process and using PGP encryption, employing the PGP public key.

6. MANAGEMENT OF REPORTED VULNERABILITIES

ZIV will manage reported vulnerabilities through a structured process, tailored to the nature and severity of each case:

Phase	Stage	Target
1	Reception and registration	Receipt of the report, identification of the affected product and collection of initial information.
2	Verification and analysis	Technical replication, validation of the finding and preliminary assessment of the impact, scope and applicability.
3	Processing	Definition of mitigation measures, compensatory measures, corrections or updates, depending on the risk and the product's life cycle.
4	Coordination and communication	Exchange of information with the notifier and the parties concerned and, where appropriate, preparation of safety notices or recommendations.
5	Follow-up and closure	Monitoring the measures taken, providing support for their implementation, and reviewing any additional information that may come to light following the notification.
6	Reception and registration	Receipt of the report, identification of the affected product and collection of initial information.
7	Verification and analysis	Technical replication, validation of the finding and preliminary assessment of the impact, scope and applicability.

The priority and timeframes for addressing issues will depend on the risk, impact, exploitability and criticality of the product, the availability of mitigations, and the complexity of the fix. ZIV will endeavour to acknowledge receipt of communications and keep the notifier informed of any relevant progress in its analysis and processing, provided that a valid means of contact has been provided and circumstances permit.

7. COORDINATED DISCLOSURE, CONFIDENTIALITY AND DATA

Reporters are asked to keep information about the vulnerability confidential whilst ZIV is analysing it and until a solution, mitigation or agreed disclosure date has been established. ZIV may coordinate with the notifier to communicate with customers, system integrators, suppliers, CERT/CSIRT or other affected parties where necessary to reduce the risk, taking into account the severity of the vulnerability, the available mitigation measures and the risks to users.

ZIV will treat the identity and contact details of the reporting party as confidential and will not publicly disclose or communicate to third parties any data that could identify them, including their name, contact details or other identifying information, nor any information that could identify their systems, networks, addresses, infrastructure or technical environment. Access to this information will be restricted to staff and parties who need to know it in order to manage the vulnerability or comply with legal obligations, and will be subject to the relevant confidentiality obligations. ZIV will not share this information outside the scope described, except where the notifier has given their express consent or where required to do so by law.

Researchers must limit the collection and retention of information to what is strictly necessary to document and report the vulnerability, and must securely delete it once it is no longer required, without prejudice to any legal obligations regarding data retention.

If, during the investigation, personal data, confidential information or trade secrets are accidentally accessed, the investigation must be halted immediately, the information must not be disclosed or used for any other purpose, and the incident must be reported to ZIV.

8. VULNERABILITIES IN THIRD-PARTY COMPONENTS

Where the issue relates to a third-party component incorporated into a ZIV solution, ZIV may coordinate the investigation and communication with the relevant supplier. If the vulnerability affects only a third-party product or service and has no specific impact on a ZIV solution, it should preferably be reported to the manufacturer or party responsible for that component, in accordance with their own disclosure policy.

9. LEGAL FRAMEWORK AND RESERVATION OF RIGHTS

This policy is intended to be consistent with best practice regarding the responsible and coordinated disclosure of vulnerabilities and does not authorize any actions that contravene applicable legislation, contractual obligations, the rights of third parties or any other applicable regulations.

Among other rules, and where applicable to the specific case, regulations on the protection of personal data, intellectual property and trade secrets must be complied with, as well as national and European regulations on the security of networks and information systems.

ZIV reserves the rights to which it is legally entitled in the event of a breach of this policy, acting in bad faith, wilful damage or unauthorized access beyond the permitted scope. ZIV may update this policy where necessary due to legal, technical, organizational or procedural changes.