

1) Purpose

Extrema is committed to managing, in a responsible and coordinated manner, any security vulnerabilities that may be identified in its products with digital elements and their related software components. This Policy defines how potential vulnerabilities may be reported to Extrema and the process adopted for their assessment, management and, where necessary, remediation.

2) Who can submit a report

Potential vulnerabilities may be reported by any natural or legal person who becomes aware of them, regardless of whether they have a contractual or commercial relationship with Extrema. Accordingly, by way of example and without limitation, reporting parties may include:

- resellers and distributors;
- installers and maintenance providers;
- product users;
- cybersecurity researchers;
- suppliers of components or services;
- companies specialising in cybersecurity;
- other entities or organisations that identify a potential vulnerability.

3) How to report a vulnerability

Reports should be submitted to the following contact:

Security contact: [security@Extrema.it]

Where available, the report should include:

- identification of the affected product;
- version of the affected product, firmware or software;
- description of the potential vulnerability;
- conditions required to reproduce the issue;
- any technical evidence or information useful for verification;
- any potential security impact;
- contact details of the reporter, if they wish to be contacted.

It is not necessary to provide information that the reporter party does not possess or cannot reasonably obtain.

4) Protection of reporting parties

Extrema will not initiate legal proceedings against anyone who reports vulnerabilities in good faith and in accordance with this Policy, provided that the research and reporting activities do not involve privacy violations, the destruction or alteration of data, or the interruption or compromise of the availability of services. This protection applies only to activities carried out in good faith and within the scope of this Policy. It does not apply to malicious, fraudulent or otherwise unlawful activities.

5) Handling of reports

Extrema will assess reports received and, where necessary, carry out technical verification of the vulnerability, assess the associated risks and identify appropriate corrective or mitigation measures. Where appropriate, Extrema will maintain communication with the reporting party throughout the vulnerability assessment and handling process.

6) Coordinated disclosure

Extrema applies a Coordinated Vulnerability Disclosure (CVD) process designed to enable the assessment and remediation of vulnerabilities before the public disclosure of technical information that could facilitate their exploitation. Information relating to a vulnerability will be shared with relevant parties on a need-to-know basis, taking into account the level of risk and applicable security requirements. Where appropriate, Extrema may coordinate the disclosure of vulnerability information with the reporting party and other relevant stakeholders.

7) Communications to users

Where a vulnerability requires action by users, installers or parties responsible for maintenance, Extrema will, where applicable, provide the necessary information and instructions and make appropriate corrective or mitigation measures available.

8) Reports relating to third-party products

Where a report concerns exclusively a third-party component or product integrated into an Extrema product, Extrema will assess the report and, where appropriate, cooperate with the relevant supplier in handling the vulnerability.

9) Contacts

For vulnerability reports:

E-mail: security@extrema.it

For requests for technical support, maintenance or warranty service, please use the standard Extrema support channels instead.