SAVOX

Procedure for vulnerability disclosure and reporting under the Cyber Resilience Act (CRA)

SAVOX

"Vulnerability Disclosure Policy

Savox Communications is committed to the security of our products and the safety of our users. We welcome and encourage security researchers, industry partners and other parties to report potential vulnerabilities in our products with digital elements.

This policy describes how to report a vulnerability and what you can expect from us.

Scope

This policy applies to all products with digital elements manufactured and placed on the market by Savox Communications, including hardware, software and associated remote data processing solutions.

Covered products are maintained in the Savox Communications Product Register and may be publicly referenced through the product catalogue available at https://www.savox.com/products

How to report a vulnerability

Please send your vulnerability report by email to: cybersecurity@savox.com

When submitting a report, please include the following information to help us assess and address the issue efficiently:

1. a description of the vulnerability and the potential security impact;
2. the affected product(s), component(s) and software version(s);
3. step-by-step instructions to reproduce the vulnerability (proof of concept); and
4. your contact details for follow-up communication.

If you wish to encrypt your report, please contact us at the email address above for encryption options.

SAVOX

What to expect

When we receive your vulnerability report, we will handle it as follows:

1. **Acknowledgement:** We will acknowledge receipt of your report and initiate our vulnerability handling process.

2. **Initial assessment:** Reported vulnerabilities will be assessed and prioritized according to their potential impact on confidentiality, integrity, availability, safety and operational resilience.

3. **Remediation:** We will work to develop and test a security update to address vulnerability without undue delay. We will keep you informed of our progress. Security updates addressing confirmed vulnerabilities will be made available to affected users in accordance with the applicable support period and product lifecycle commitments.

4. **Disclosure:** We follow a coordinated vulnerability disclosure approach. We ask that you do not publicly disclose the vulnerability until we have had a reasonable opportunity to develop and release a corrective measure. We will coordinate the timing of any public disclosure with you. The disclosure timeline will be agreed between Savox Communications and the reporter based on severity, exploitability and remediation complexity.

Safe harbor

Savox Communications will not take legal action against individuals who report vulnerabilities in good faith and in compliance with this policy. We consider good-faith security research conducted in accordance with this policy to be authorized and will not pursue civil or criminal action in connection with such research, provided that the reporter:

a. does not exploit the vulnerability beyond what is necessary to demonstrate the security issue;

b. does not access, modify or delete data belonging to others;

c. does not disrupt or degrade the availability of our products or services; and

d. complies with all applicable laws.

Contact

Email: cybersecurity@savox.com

The Cyber Security Team acts as the vulnerability management and coordinated disclosure function for Savox Communications.
This policy is maintained by the Savox Communications Cyber Security Team and was last updated on 11.9.2026."