Sep 11, 2026

SiteWorx Coordinated Vulnerability Disclosure Policy

Policy Overview

At SiteWorx (siteworx.io), cybersecurity and hardware integrity are fundamental to our operations. We recognize the vital role that independent security researchers, customers, and the broader global white-hat community play in identifying vulnerabilities.

This document describes our policy for informing customers and partners of potential security vulnerabilities in supported products and services.

Scope

Scope This policy covers all commercial products and connected services made available by SiteWorx, in accordance with the EU Cyber Resilience Act (Regulation EU 2024/2847).

Out-of-scope assets:

- **Physical & Social Engineering**: Physical access attacks on SiteWorx facilities, offices, or personnel, as well as phishing, or social engineering.
- **Service Disruption**: Any form of Denial of Service (DoS/DDoS) attack intended to exhaust system resources or disrupt physical hardware and cloud services.
- **Low-Impact Web Flaws**: Missing non-critical HTTP response headers without a demonstrated exploit path, or CSRF on non-sensitive, public forms.
- **Third-Party Systems**: Independent third-party cloud applications, external APIs, or upstream software components not directly maintained or customized by SiteWorx.

Safe Harbor

SiteWorx permits individuals to conduct non-commercial security research and testing on our hardware, firmware, and cloud services, provided such activities are performed in good faith to

identify, analyze, or remediate potential security vulnerabilities.

SiteWorx will not initiate or support legal action against any researcher who makes a genuine, good-faith effort to adhere to our Coordinated Vulnerability Disclosure (CVD) process and complies with all applicable local and international laws.

This authorization strictly excludes any security testing that disrupts, degrades, or damages SiteWorx devices, software, or infrastructure, or is conducted with malicious intent or in bad faith. Furthermore, this safe harbor protection does not extend to unauthorized security testing performed on third-party services, external APIs, or upstream dependencies integrated with SiteWorx products.

Reporting Channel & Submission Requirements

Please submit all discovered security issues directly to our monitored security intake:

- **Primary Email**: security@siteworx.io
- **RFC 9116 Metadata**: Accessible directly at https://siteworx.io/.well-known/security.txt

Submission Checklist

To assist our engineering team in triaging your report quickly, please include:

1. **Target Identification**: Device model (e.g., SGW1), firmware version, build tag, or specific cloud API endpoint.
2. **Vulnerability Classification**: Category (e.g., Remote Code Execution, Privilege Escalation, Command Injection).
3. **Reproduction Steps**: Step-by-step instructions or proof-of-concept scripts to reproduce the vulnerability safely.
4. **Impact Assessment**: Your analysis of how an attacker could leverage the flaw and its potential operational impact.
5. **Attribution**: Your name, handle, or organization for public credit (or explicitly note if you prefer to remain anonymous).

Regulatory Compliance

SiteWorx complies with the **European Union Cyber Resilience Act** (Regulation EU 2024/2847).

- **Mandatory Disclosure**: Under Article 14 of the CRA, if a reported vulnerability is determined to be actively exploited in the wild, SiteWorx is legally required to notify

the European Union Agency for Cybersecurity (ENISA) and relevant national Computer Security Incident Response Teams (CSIRTs) via the ENISA Single Reporting Platform (SRP).

- **Reporting Schedule**: This regulatory process operates on a multi-stage timeline: an Early Warning within 24 hours of confirmed active exploitation awareness, a Detailed Notification within 72 hours, and a Final Report within 14 days of patch availability.
- **Independent Execution**: Regulatory filings to ENISA operate independently of our direct coordination commitments with reporting researchers.