Coordinated Vulnerability Disclosure Policy

Public policy for reporting and coordinating security vulnerabilities

This policy explains how SKYWORTH receives, evaluates, remediates and discloses security vulnerabilities reported in its information systems, products, services and supported equipment. It is intended for external security researchers, customers, partners and other parties who wish to report a potential vulnerability responsibly.

1. Scope

This policy applies to reports concerning:

- software and hardware products developed by SKYWORTH, including firmware, client software and server-side components;
- SKYWORTH's internal business information systems;
- cloud and SaaS services provided by SKYWORTH; and
- hardware, software and related support systems deployed in cooperation with SKYWORTH.

It applies to all external individuals, research institutions, security vendors, customers and other parties that report a security vulnerability (each a "Reporter"), and to all Company personnel involved in vulnerability handling.

2. References and governing principles

This policy is informed by ISO/IEC 29147:2018 (Information technology — Security techniques — Vulnerability disclosure), EN 40000-1-3 where applicable, the applicable requirements of Regulation (EU) 2024/2847 (the Cyber Resilience Act, or "CRA"), and other applicable laws, regulations and sector-specific security requirements.

3. How to report a vulnerability

Vulnerability reporting form: Please use the security vulnerability reporting form published on this website: https://www.solavita.com/index.php?s=/En/Index/pageView/catid/74.

Security contact: Please use the security contact details published on this website: security@solavita.com or via this number 400-900-9016. Reports submitted through official channels are handled using secure HTTPS or encrypted email, as applicable.

Our reporting channels support multiple access methods so that people with writing or other accessibility limitations can submit information and request assistance.

4. Information to include in a report

To help us validate and remediate a report quickly and accurately, please provide complete, accurate and current information, including:

- Reporter details — your name or organization, a reliable email address and/or telephone number, and your organization (if any). Anonymous reports should include at least one channel through which we can provide feedback.
- Affected asset — the exact product, system or device name, model, version, deployment environment, affected function or module, and access path.
- Vulnerability details — the vulnerability type (for example, remote code execution, SQL injection, privilege escalation or information disclosure), trigger conditions, reproducible steps, required network conditions and required privileges.
- Validation material — screenshots, tool output, network captures, system logs or a minimal proof of concept that demonstrates the issue. Do not submit destructive exploitation tools, malware or other material that could harm systems or data. Include the observed or reasonably foreseeable security impact.

- Additional context — discovery date, whether the issue has been disclosed to any third party, any proposed remediation, and other relevant information.

By submitting a report, the Reporter confirms that the information is accurate to the best of their knowledge, that the vulnerability was not used to conduct an attack, and that vulnerability details will not be disclosed to third parties before remediation is completed, unless otherwise agreed with SKYWORTH or required by law.

5. Our vulnerability handling process

SKYWORTH follows a standardized, closed-loop process for every report:

- Monitoring and triage — the security response team monitors official reporting channels 24/7 and performs an initial screening to determine whether a report contains a potentially valid security vulnerability.
- Acknowledgement — for a valid report, we will send an acknowledgement within two business days, identify the point of contact, provide contact details and explain the next steps. If a report is not accepted, we will provide the reason where practicable and close the handling process.
- Technical assessment — we reproduce the issue where possible, assess exploitability and impact, assign a risk level, identify affected versions and coordinate a remediation plan with the responsible product and engineering teams.
- Remediation and verification — we develop and test a patch, update or mitigation, verify that it addresses the vulnerability, and track the result in the vulnerability record.
- Downstream communication — once a patch has been verified, we proactively notify affected downstream integrators and end users as appropriate. Communications and evidence are retained in the CRA technical documentation package where applicable, and relevant instructions, patches and temporary mitigations are reflected in the product installation documentation.

A report may be closed as not accepted where the issue cannot be reproduced and no further useful evidence is available; it is a duplicate; it affects a product that has been retired and is no longer supported; it is not a security vulnerability or the report does not establish a security impact; or another documented reason makes the report invalid. A closure decision does not prevent the Reporter from submitting additional evidence for reconsideration.

6. Confidentiality and coordination periods

During the intake and coordination phase, SKYWORTH will assess the severity, scope and remediation difficulty and agree an appropriate confidentiality period with the Reporter where practicable. Unless otherwise agreed:

- High-risk vulnerabilities: a target coordination period of 90 days.
- Medium-risk vulnerabilities: a target coordination period of 60 days.
- Low-risk vulnerabilities: a target coordination period of 30 days.

Vulnerability information is restricted during the coordination period and must not be disclosed prematurely. These target periods do not delay mandatory regulatory reporting, emergency user warnings or other action required to protect users.

7. Public disclosure

SKYWORTH follows the principles of ISO/IEC 29147:2018 and applicable CRA requirements when deciding whether and when to publish vulnerability information. We disclose only information necessary to protect users and provide a fix; we do not publish exploit instructions, core source code, proof-of-concept files or other sensitive details.

7.1 Disclosure authority

SKYWORTH is the sole authorized publisher of public vulnerability notices. No department or individual may disclose vulnerability information externally without authorization.

7.2 Timing

Routine disclosure: After remediation has been completed and verified, we will publish a formal security advisory through official channels within three business days. The advisory will describe the affected products, the security impact at an appropriate level and the available remediation.

Emergency disclosure: If a vulnerability has been unlawfully disclosed, is at risk of widespread malicious exploitation, or must be disclosed earlier because of regulatory or legal requirements, we will take necessary temporary protective measures and publish a warning within 24 hours. The warning will explain the risk and temporary protections. A complete remediation notice will follow when the fix is available.

Delayed disclosure: If immediate disclosure could create a material risk to a core business system, disclosure may be delayed following a documented risk assessment and approval by SKYWORTH's information security lead, and after seeking the Reporter's understanding where practicable. The delay must not exceed seven business days after remediation is completed, and we will keep the Reporter informed of progress.

8. Follow-up after disclosure

SKYWORTH maintains a user feedback record, answers questions about remediation, assists users with applying fixes and follows up on remediation status. If a vulnerability is found to be reproducible in additional environments or a new exploitation method is identified, we will promptly initiate incident response and update the relevant advisory.

9. Prohibited conduct

SKYWORTH may terminate coordination immediately and reserve all civil, administrative and criminal remedies if a Reporter:

- knowingly submits false vulnerability information or intentionally disrupts SKYWORTH's security work;
- violates the agreed confidentiality period or discloses vulnerability details to a third party or the public before remediation is completed;
- uses a reported vulnerability to attack systems, obtain Company or user data, or disrupt normal operations;
- discloses sensitive internal information provided during vulnerability handling;
- demands money or makes unreasonable demands in connection with a report, or uses threats, coercion or similar conduct to interfere with remediation; or
- breaches another obligation under this policy and refuses to correct the breach after being asked to do so.

Where prohibited conduct causes loss to SKYWORTH or its users, SKYWORTH may seek compensation as permitted by applicable law.

10. Policy updates

SKYWORTH may update this policy to reflect changes in products, services, law or security practice. The current version published on this website is the version that applies to new reports.