Coordinated Vulnerability Disclosure (CVD) Policy

ShenzhenWinline Technology Co., Ltd. — EV Charging Products with Digital Elements

Version 1.0 | Effective date: 2026-12-01 (draft for publication) | Status: PUBLIC

This policy sets out how Winline receives, handles and discloses reports of security vulnerabilities in its products and services. It is published in accordance with Article 13(8) and Annex I, Part II(5) of the EU Cyber Resilience Act (Regulation (EU) 2024/2847), and aligns with ISO/IEC 29147:2014 (Vulnerability Disclosure) and ISO/IEC 30111 (Vulnerability Handling), ENISA guidance on coordinated vulnerability disclosure, and the RFC 9116 security.txt standard.

Applies from: this CVD programme is operated today on a voluntary basis and becomes a regulatory obligation for products placed on the EU market from 11 December 2027 under CRA Article 13(8); the Article 14 regulatory reporting duty (ENISA SRP) has applied since 11 September 2026.

1. Purpose and Scope

Winline designs, manufactures and operates EV charging equipment (AC and DC chargers, charging modules). Because these are 'products with digital elements' within the meaning of the CRA, and the security-relevant elements are the network-relevant components embedded within the charging stations (such as the OCPP client on the charger side, the charging controller and the local network interfaces), Winline operates a Coordinated Vulnerability Disclosure (CVD) programme so that security researchers, customers, partners and suppliers can report potential vulnerabilities affecting those components in a structured, responsible manner, and so that confirmed vulnerabilities are remediated and disclosed on a coordinated timeline. Winline does not itself provide a mobile application or a cloud/backend service; where a charging station connects to a customer- or third-party-operated backend (e.g., via OCPP), only the charger-side implementation is covered by this policy.

In scope: all Winline-branded EV charging stations and charging modules (with model/version identifiers) placed on the EU market, and the network-relevant components embedded within them — including the OCPP client implementation on the charger side, the charging controller, and the local network interfaces (e.g., Ethernet, Wi-Fi, cellular); the firmware/software delivered with the products is likewise in scope. Products that have reached end-of-support are listed in our support-lifecycle statement; reports for end-of-life products are accepted but response timelines may differ. Backend/cloud platforms and mobile applications operated by customers or third parties are outside Winline's scope.

Out of scope / not authorised under this policy: physical tampering or testing of deployed equipment without authorisation; social engineering against Winline staff or customers; denial-of-service (DoS) testing against production systems; brute-force or high-volume automated scanning that degrades service; accessing, modifying or deleting data beyond what is strictly necessary to demonstrate the vulnerability; and introduction of malware. Good-faith research that stays within the boundaries below is authorised and protected by the Safe Harbor in Section 7.

2. How to Report a Vulnerability

Winline designates a single point of contact (SPOC) for vulnerability reports, consistent with CRA Article 13 language. Reports may be submitted by any of the following channels. Encrypted submission is strongly recommended.

Preferred channel (fastest acknowledgement):

- Email: security@szwinline.com
- PGP-encrypted email: our public PGP key (fingerprint [PLACEHOLDER — e.g. XXXX…XXXX]) is published at https://en.szwinline.com/security/pgp-key.asc and referenced in security.txt.
- Machine-readable contact: a security.txt file is published at https://en.szwinline.com/.well-known/security.txt (RFC 9116).
- Anonymous reports are accepted — researchers may withhold their identity.

Information to include:

- Affected product name, model and firmware/software version.
- A clear description of the vulnerability and its potential impact.
- Step-by-step reproduction instructions and, where available, proof-of-concept (PoC), screenshots or logs.
- CWE category, if known.
- Whether you believe the vulnerability is already being actively exploited.
- Your proposed disclosure plan / preferred embargo period.

Note: automated scanner output without validation, or reports that do not allow reproduction, may not be actioned. If you inadvertently access personal data, notify us promptly.

3. Our Commitments and Response Timeline

Winline PSIRT commits to the following milestones from Day 0 (the date a well-formed report is received). Timelines may be extended for complex vulnerabilities affecting multiple products or upstream components; any extension will be communicated proactively to the reporter.

Milestone	Commitment
Acknowledgement of receipt	Within 48 hours (2 business days) of receipt, a personal acknowledgement (not an auto-reply only) is sent.
Initial severity assessment	Within 5 business days: validate, assign a risk level, check for duplicates, set a remediation target.
In-scope determination & plan	Communicate whether the report is in scope and the planned remediation timeline.
Progress updates	Regular updates (at least every 10 business days) until the issue is resolved.
Coordinated disclosure date	Agreed with the reporter; default embargo ~90 days from report, shortened if actively exploited.
Security advisory publication	Published upon patch availability, in human-readable (SA) and machine-readable (CSAF) form.

Target patch availability by risk level, measured from confirmation of the fix: High (including actively exploited or Critical cases) within 7 days; Medium within 30 days; Low within 60 days. Cases that are actively exploited or constitute a significant incident additionally trigger the Article 14 emergency reporting timeline (24h / 72h / 14d) described in Section 8. Winline PSIRT tracks these patch SLAs together with the milestones above.

4. Severity Assessment

Winline grades the severity of each confirmed vulnerability using a risk-level framework aligned with the EU Cyber Resilience Act (Regulation (EU) 2024/2847, Article 6). Article 6 establishes a three-tier risk classification for products with digital elements — High Risk (Class II), Medium Risk (Class I) and Low Risk (Unclassified / Default), in descending order of risk. For every report, Winline: (a) maps the affected charging product and its network-relevant components (the OCPP client on the charger side, the charging controller, and the local network interfaces) to the applicable CRA risk tier; (b) assigns the vulnerability a risk level — High, Medium or Low — based on its potential impact on confidentiality, integrity and availability, its exploitability, and the exposure of the affected component; and (c) uses that risk level to set prioritisation, the remediation target date, and whether the Article 14 regulatory incident-reporting duty is triggered. Winline's EV charging products are mapped to this official CRA classification to determine the applicable conformity assessment and obligation tier.

5. Coordinated Disclosure and Embargo

Winline practices coordinated disclosure: the vulnerability is handled privately, a remediation is developed, and the advisory is published alongside or shortly after the fix. The default embargo is approximately 90 days from the report date; it may be shortened where the vulnerability is already being actively exploited, and may be extended for genuinely complex, multi-party cases (documented with rationale). Long embargoes are avoided because attackers can independently find the same flaw.

Both Winline and the reporter undertake to keep vulnerability details confidential until public disclosure, except where disclosure is required by law or coordinated through a national CSIRT.

6. Public Disclosure of Fixed Vulnerabilities

Once a security update is available, Winline publicly discloses information about the fixed vulnerability, in line with Annex I, Part II(4) of the CRA. Each advisory (Security Advisory, 'SA') includes: affected product and versions, a description of the vulnerability, its severity/impact, risk level, clear remediation/mitigation steps, references (CVE ID where assigned), and the publication date. Advisories are published on the Winline Security Advisories page and, where technically feasible, also provided in machine-readable CSAF 2.0 format and via an RSS feed. The narrow exception (delayed disclosure where the security risk of publication outweighs the benefit) is applied only until users have had the opportunity to apply the patch. In addition, as required by the CRA, information on fixed vulnerabilities is also made available through the EU Vulnerability Database (EUVD).

7. Safe Harbor and Legal Commitment

Winline will not pursue legal action against researchers who, in good faith, follow this policy. Authorised good-faith activities include testing within the stated scope, accessing only the minimum data needed to demonstrate a vulnerability, and responsibly reporting findings. We will credit researchers (by name or alias, with their consent) in the published advisory.

Prohibited activities (no safe harbor): accessing, modifying or deleting data belonging to others; disrupting or degrading Winline charging equipment or the charging services of its customers; social engineering; physical tampering with deployed equipment; introducing malware; or any activity that violates applicable law. Reports must not include personal data beyond what is strictly necessary.

8. Regulatory Reporting — ENISA Single Reporting Platform (Article 14)

Where a vulnerability in a Winline product is being actively exploited, or constitutes a significant incident, Winline reports to the EU through ENISA's Single Reporting Platform (SRP) as required by CRA Article 14: an early warning within 24 hours of becoming aware, a detailed notification within 72 hours, and a final report within 14 days of a fix or mitigation being available. This regulatory duty has applied since 11 September 2026. The same SPOC channel that receives researcher reports feeds Winline's internal triage and, where applicable, the ENISA notification process. Public disclosure of fixed vulnerabilities is separately handled via advisories and the EU Vulnerability Database (EUVD) as described in Section 6.

9. Third-Party and Multi-Party Coordination

If a reported vulnerability also affects products of other vendors or upstream components, Winline will coordinate disclosure through the relevant national CSIRT designated as coordinator (under NIS2 Article 12 / CRA Article 14), or via a recognised CERT, to protect downstream users. Where a third-party component is affected, Winline reports the vulnerability to the component's maintainer and, where appropriate, shares the remediation in machine-readable form (CRA Article 13(6)).

10. Researcher Recognition

With the reporter's explicit consent, Winline acknowledges the researcher's contribution in the published advisory and, where appropriate, in a public Hall of Recognition. Consent is recorded separately from the technical report so that anonymity is always respected.

11. Contact and Security Indicators

- Vulnerability reports (SPOC): security@szwinline.com
- PGP public key: https://en.szwinline.com/security/pgp-key.asc (fingerprint [PLACEHOLDER])
- security.txt: https://en.szwinline.com/.well-known/security.txt
- Security Advisories: https://en.szwinline.com/security/advisories/
- General security information: https://en.szwinline.com/security/

12. Review and Version Control

This policy is reviewed at least annually and updated to reflect regulatory changes (including CRA harmonised standards under Mandate M/606) and lessons learned. Version history is retained for audit readiness.

13. Languages and Legal Effect

This policy is published on Winline's official website in English, which is the authoritative and legally operative version.In the event of any inconsistency between the language versions, the English version prevails. Nothing in this policy limits Winline's obligations under applicable law, nor does it create a contractual right for any third party.

Note: the Chinese text is a non-binding translation prepared for convenience only; the official, publicly posted version is English.

DRAFT FOR INTERNAL REVIEW — before publication, replace the remaining [PLACEHOLDER] items (PGP fingerprint; confirm the domain en.szwinline.com and the security pages/URLs are live), confirm the effective date, and have legal counsel verify the Safe Harbor and Article 14 statements against the latest CRA texts and the company's nominated Member-State reference and Authorised Representative.