Coordinated Vulnerability Disclosure Statement

Version: V1.0

Effective Date: 2026-08-15

Compliance Basis: EU CRA Regulation (EU) 2024/2847

1. Overview

In compliance with the EU Cyber Resilience Act (CRA) and EN 40000-1-3 cybersecurity standards, the Company establishes a standardized Coordinated Vulnerability Disclosure (CVD) mechanism. This public statement standardizes the full process of vulnerability reception, response, remediation and public disclosure, ensuring full compliance for all networked smart display products sold in the EU market.

2. Vulnerability Reporting Channel (7×24h)

Official Security Email: security@expressluck.com

Public Access Path: https://www.smarttech-tv.com/cybersecurity-policy

Security researchers, users and third-party institutions are welcome to submit product security vulnerabilities through the official channel.

To better respond the issues you raised, please provide the information including product model, SN number, description of safety issues etc.

3. Official Response Commitment

1. Acknowledge all valid vulnerability reports within 48 hours;

2. Verify vulnerability authenticity and conduct CVSS risk grading based on product SBOM;

3. Release firmware patches for high-risk vulnerabilities and provide official mitigation solutions if immediate patches are unavailable;

4. Publish official security advisories after vulnerability remediation.

4. EU CRA Compliance Commitment

For products placed on the EU market, the Company fully complies with CRA Article 14 mandatory notification obligations effective from 11 September 2026:

1. Submit mandatory notifications via ENISA SRP platform once actively exploited vulnerabilities or severe cybersecurity incidents are confirmed;

2. Complete 24-hour early warning, 72-hour full notification and 14-day final report in strict accordance with legal time limits;

3. Retain full vulnerability lifecycle records for no less than 10 years to meet EU market supervision and traceability requirements.

5. Disclosure Policy

To prevent widespread security risks, vulnerability details will not be publicly disclosed before official patches and mitigation measures are released. The Company will publicly disclose relevant vulnerability information after remediation to continuously improve product cybersecurity performance.

6. Compliance Declaration

This CVD mechanism fully meets the mandatory requirements of EU CRA (EU) 2024/2847 and EN 40000-1-3:2025, serving as valid public compliance evidence for EU market access, technical document review and market supervision inspection.

7.Others

To better respond the issues you raised, please provide the information including product model, SN number, description of safety issues etc.