Coordinated Vulnerability Disclosure Policy

Organization :	CINCOZE
Version :	V1.0
Date :	2026/07/30
Contact :	[cra@cincoze.com](mail to:cra@cincoze.com)
By :	Jessica Chiang

Document Revision History

Reversion	Date	Revision Reason	Description of Changes	Revised By
1.0	2026/07/30	New Release	New Release	Jessica Chiang

Item Details

No.	Item	Description
1.	Scope	This Policy applies to all products and connected hardware devices manufactured, distributed, or maintained by CINCOZE and placed on the European Union market in accordance with Regulation (EU) 2024/2847 (Cyber Resilience Act).
2.	How to Report a Vulnerability	We encourage security researchers and users who discover potential vulnerabilities to report them responsibly before publicly disclosing any vulnerability details. **Reporting Channels** Please use one of the following methods to contact our Product Security Incident Response Team (PSIRT): **Encrypted Communications:** If your report contains sensitive information, we recommend encrypting your email using PGP. Our public key is available for download at: https://www.cincoze.com/Download/pgp/cincoze-cra-public.asc Please provide the following information: - A clear description of the vulnerability and its potential impact; - The affected product(s) and version(s); - Steps to reproduce the vulnerability or a proof of concept (PoC), where it can be safely shared; and - Your preferred contact information for follow-up.
3.	Our Commitment to Reporters	CINCOZE commits to: - Acknowledge receipt of your vulnerability report within **5 business days**; - Provide an initial assessment within **15 business days**; - Keep you regularly informed of the progress of our investigation and remediation; - Credit your contribution in the security advisory, unless you request to remain anonymous; and - Not take legal action against security researchers who report vulnerabilities in good faith and in accordance with this Policy.

Item Details

No.	Item	Description
4.	Coordinated Disclosure Timeline	**Coordinated Disclosure Timeline** CINCOZE follows the vulnerability disclosure and handling processes outlined in **ISO/IEC 29147** and **ISO/IEC 30111**. ISO/IEC 29147 describes the external **Coordinated Vulnerability Disclosure (CVD)** process, while ISO/IEC 30111 covers the internal processes for vulnerability handling and response. CINCOZE follows the principles of Coordinated Vulnerability Disclosure and will coordinate the public disclosure timeline with the reporter once remediation measures are ready. If remediation cannot be completed within the coordinated disclosure period due to technical complexity, dependencies on third-party components, or supply chain factors, CINCOZE will proactively explain the reasons to the reporter and negotiate an extension. The disclosure period may be extended upon mutual agreement between CINCOZE and the reporter. If remediation remains incomplete when the extended period expires and the parties cannot reach an agreement on a further extension, CINCOZE will issue a security advisory in accordance with the agreed timeline and provide recommended mitigation measures. Public disclosure will not be further delayed solely because remediation has not been completed. CINCOZE may also make an earlier disclosure under the following circumstances: the vulnerability has already been publicly disclosed by a third party, there is evidence that the vulnerability is being actively exploited, or CINCOZE and the reporter mutually agree to earlier disclosure. - We will remediate the vulnerability within the agreed timeline. - If remediation requires additional time, we will work with the reporter to negotiate an extension. - If the vulnerability has been publicly disclosed or is being actively exploited, we may accelerate the disclosure timeline.

Item Details

No.	Item	Description
5.	CRA Reporting Obligations	If CINCOZE determines that a reported vulnerability is being actively exploited, CINCOZE is required under **Article 14 of Regulation (EU) 2024/2847 (Cyber Resilience Act)** to: - Submit an early warning notification to ENISA and the CSIRT designated as coordinator within 24 hours of becoming aware of the vulnerability; - Submit a vulnerability notification within 72 hours of becoming aware of the actively exploited vulnerability; - Submit a final report to ENISA and the relevant CSIRT designated as coordinator no later than 14 days after a corrective or mitigating measure becomes available. For the purposes of the preceding paragraph, a corrective or mitigating measure is considered available when the earliest of the following occurs: 1. A security patch, firmware update, or software update has been officially released and made available to affected users; or 2. CINCOZE has officially published an effective mitigation measure, configuration change guidance, or temporary workaround that reduces the risk associated with the vulnerability. If corrective or mitigating measures cannot be completed within a reasonable period due to technical or supply chain factors, CINCOZE will provide status updates as required and submit the final report within the applicable period once the corrective or mitigating measure becomes available. - CINCOZE will also timely notify affected users where required. Initiating a coordinated vulnerability disclosure process with the reporter does not exempt CINCOZE from, or delay, these reporting obligations.
6.	Out of Scope	The following activities and issues are not within the scope of this Policy: - Denial-of-Service (DoS) attacks against our infrastructure; - Social engineering or phishing attacks targeting our employees; - Vulnerabilities in third-party services that are outside of our control; and - Physical attacks that require on-site access.

Item Details

No.	Item	Description
7.	Safe Harbor	CINCOZE will not initiate civil or criminal legal action against security researchers who meet all of the following conditions: - Act in good faith and comply with this Policy; - Do not access, modify, or delete data unless strictly necessary to demonstrate the existence of the vulnerability; - Do not exploit the vulnerability beyond what is necessary to confirm its existence; - Do not disrupt CINCOZE' s production systems or compromise customer data; and **- Refrain from publicly disclosing any details of the vulnerability until the earlier of (i) CINCOZE has remediated the vulnerability and published a security advisory, or (ii) the disclosure period specified in Section 4, including any mutually agreed extension, has expired.**
8.	References	- Regulation (EU) 2024/2847 (Cyber Resilience Act), Article 14 - ENISA Single Vulnerability Reporting Platform：https://www.enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp - RFC 9116 (security.txt)：https://www.rfc-editor.org/rfc/rfc9116

cincoze

Expertise in Embedded Computing