協調漏洞揭露政策

(Coordinated Vulnerability Disclosure Policy)

組織：	CINCOZE
版本：	V1.0
生效日期：	2026/07/30
聯絡方式：	[cra@cincoze.com](mail to:cra@cincoze.com)
撰寫：	Jessica Chiang

文件變更履歷

版本	日期	修訂原因	修訂內容	修訂者
1.0	2026/07/30	新建立	新建立	Jessica Chiang

項目內容

No.	項目	說明
1.	適用範圍	本政策適用於所有由 CINCOZE 製造、分銷或維護，並根據歐盟法規 (EU) 2024/2847（網路彈性法案）投放歐盟市場的軟體產品和連網硬體設備。
2.	如何回報漏洞	我們鼓勵發現潛在漏洞的安全研究人員和用戶在公開披露之前，以負責任的方式報告漏洞。 **通報管道 (Reporting Channels)** **請選擇下列任一方式聯繫我們的產品安全事件回應團隊 (PSIRT)** **電子郵件： 將詳細資料寄送至 cra@cincoze.com。** **加密通訊： 若通報內容涉及敏感資訊，建議使用 PGP 加密您的電子郵件。我們的公開金鑰可至** https://www.cincoze.com/Download/pgp/cincoze-cra-public.asc **下載。** 請提供以下資訊： - 漏洞及其潛在影響的清晰描述 - 受影響的產品及版本 - 重現步驟或概念驗證（如安全性可分享） - 您希望我們跟進的聯絡方式
3.	我們對報告者的承諾	CINCOZE 承諾： - 在**5 個工作天**內確認收到您的報告 - 在**15 個工作天**內提供初步評估 - 定期向您通報進度 - 在安全公告中註明您的貢獻（除非您要求匿名） - 不會對根據本政策善意報告的研究人員採取法律行動

項目內容

No.	項目	說明
4.	協調揭露時間表	**協調揭露期限** **本公司採 ISO/IEC 標準 29147 漏洞揭露與 30111 漏洞處理程序，ISO/IEC 29147 描述了對外的CVD流程 ，ISO/IEC 30111 則涵蓋漏洞回應相關的內部流程。** **本公司採協同漏洞揭露原則，於修補措施備妥後與通報者協調公開揭露時程。** **若因技術複雜度、第三方元件相依性或供應鏈因素致修補無法於協同漏洞揭露期限內完成，本公司將主動向通報者說明原因並協商延長。經雙方同意者，得延長揭露期限。** **若延長期限屆滿修補仍未完成，且雙方無法就進一步延長達成共識，本公司將依約定期限發布安全公告並提供緩解措施建議，不因修補尚未完成而延後揭露。** **本公司亦得於下列情形提前揭露：該漏洞已遭第三方公開、已有證據顯示遭積極利用，或經雙方同意提前公開。** - 我們將在規定期限內修復漏洞。 - 如果修復需要更長時間，我們將與報告者協商延期。 - 如果漏洞已被公開或正在被積極利用，我們可能會加快揭露。

項目內容

No.	項目	說明
5.	CRA 報告義務	如果確定已報告的漏洞正在被積極利用，根據 (EU) 2024/2847 號條例第 14 條，CINCOZE 有義務： - 在知悉漏洞後 24 小時內向 ENISA 提交**預警** - 在 72 小時內提交**詳細通知** **- 本公司將於針對該漏洞之矯正措施或緩解措施可供使用之日起 14 日內，向 ENISA 及相關國家 CSIRT 提交最終報告。** **前項所稱「可供使用」，指下列情形之一最早發生者：** **（一）修補程式、韌體更新或軟體更新已正式釋出並可供受影響使用者取得；** **（二）本公司已正式發布可有效降低該漏洞風險之緩解措施、設定變更指引或暫時性因應方案。** **若因技術或供應鏈因素致矯正措施無法於合理期間內完成，本公司將依規定提交進度說明，並於措施可供使用後依前項期限提交最終報告。** - 及時通知**受影響的使用者** 與我們啟動協調揭露並不免除或延緩這些義務。
6.	超出範圍	以下內容**不**屬於本政策的適用範圍： - 針對我們基礎設施的拒絕服務攻擊 - 針對我們員工的社會工程或網路釣魚攻擊 - 我們無法控制的第三方服務中的漏洞 - 需要現場訪問的實體攻擊

項目內容

No.	項目	說明
7.	安全港條款	CINCOZE 不會對符合以下條件的安全研究人員提起民事或刑事訴訟： - 秉持誠信並遵守本政策 - 除為證明漏洞所絕對必要外，不得存取、修改或刪除數據 - 除確認漏洞存在外，不得利用漏洞 - 未破壞德承正式營運系統與客戶資料 **- 於本公司完成修補並發布安全公告前，或於前述第4項所訂揭露期限（含經協商之延長期間）屆滿前，以先屆至者為準，敬請通報者暫不自行公開揭露該漏洞之相關細節。**
8.	參考資料	- (EU) 2024/2847 號條例（網路彈性法），**第14條（Article 14）** - ENISA 單一報告平台：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