動力安全資訊股份有限公司

Dynasafe Technologies Inc.

Dynasafe

EMILY.RPA 弱點分析報告

目錄 Agenda

- 執行摘要
- 分析方法
- 分析結果
- 分析圖示
- 弱點掃描附件

執行摘要

弱點掃描與分析報告摘要

- 本報告係基於動力安全公司於研發環境中建置之資安弱點測試平台,於2026年8月7日分別對 EMILY.RPA軟體執行弱點掃描與安全分析後所產出之結果。
- 動力安全公司研發人員依據EMILY.RPA軟體之作業需求,先行建立測試系統環境,並依標準安裝程序完成EMILY.RPA之部署,隨後啟動本次弱點掃描與分析作業。
- 掃描與分析工具採用具國際公信力之Tenable Nessus,對EMILY.RPA軟體進行前後比對與綜合分析。經分析結果顯示,未發現任何已知或具潛在風險之安全弱點,系統運作正常、安全防護良好。
- 若需進一步瞭解動力安全公司於本次弱點掃描中所採用的分析方法、檢測流程,或針對EMILY.RPA的詳細技術分析結果與對應修正建議,請參閱本報告後續章節與附件之詳細說明。

分析方法

弱點分析程序說明

本次分析程序係依據動力安全公司所建置之弱點分析基礎架構進行,目的在於驗證 EMILY.RPA 軟體於實際運行環境中的資訊安全性與穩定性。整體弱點分析基礎架構與程序如下:

- 分析環境與工具
  - 本次測試於 Windows Server 2025 平台中執行,系統環境安裝EMILY.RPA Server 4.1.20260809 版本,並搭配 EMILY.RPA Client 4.1.20260809 版本 以模擬實際運作條件。弱點掃描與分析工具採用Tenable Nessus Version 10.12.1,執行完整的系統與應用層安全檢測。
- 測試程序
  - 完成 EMILY.RPA Server 4.1.20260809 / Client 4.1.20260809安裝與系統配置後,立即啟動 Tenable Nessus Version 10.12.1進行全面性弱點掃描,針對作業系統、應用服務及網路通訊埠進行檢測與分析。
- 分析目的
  - 本次測試旨在確認 EMILY.RPA 於正式運行環境下之資訊安全防護狀況,確保軟體安裝後無新增高風險或可被利用之安全弱點。

分析結果

INFO說明

- 經本次弱點掃描與安全分析驗證結果顯示，EMILY.RPA軟體運作穩定、安全防護完善，已通過測試環境之驗證要求，可安心部署並執行於企業客戶所使用之測試與開發環境中。

- 經Tenable Nessus 專業分析工具進行全面性掃描後，未發現與EMILY.RPA相關之安全弱點或潛在風險。此結果再次證實EMILY.RPA為具備高度安全性與可信任度的企業級應用軟體。

分析圖示

2026年8月7日掃描結果

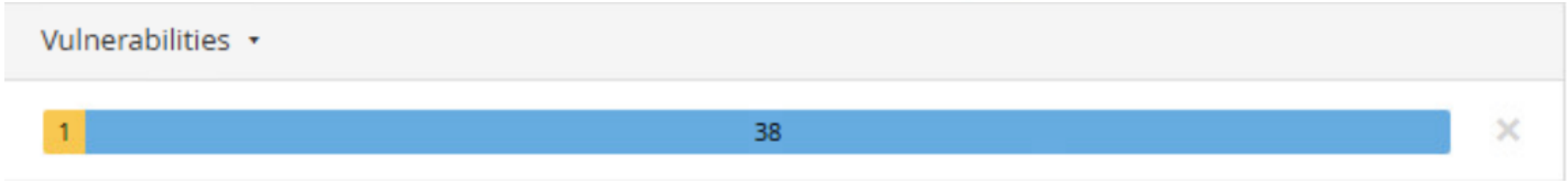
- tenable Nessus

Scan Details EMILY.RPA

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info



弱點掃描說明

弱點說明

本次針對 EMILY.RPA 系統進行的弱點掃描結果顯示,所有檢測項目均未發現任何 高風險(High)或中風險(Medium)的安全弱點。

整體掃描結果僅包含一項低風險(Low)此弱點是作業系統對於ICMP Timestamp的回應，與EMILY.RPA應用無關，且可以使用防火牆作為防禦手段而消除此項弱點，其他的資訊性(Informational) 項目屬於作業系統與環境設定的提示資訊,**並不代表實際存在安全威脅或漏洞**。

資訊性項目(Info)為Nessus掃描工具自動偵測應用程式服務版本、通訊協定回應、或作業系統組態時所產生的記錄,目的在提供管理者更完整的系統資訊以利後續維護與監控。**此類訊息不具風險層級,亦不會影響系統安全性或穩定性**。

經資安顧問綜合分析後,確認:

□ 系統整體未發現可被利用的安全漏洞或弱點。
□ 未開放外部未授權連線或服務埠。
□ 作業系統防護機制(防火牆、服務權限、網路隔離等)運作正常。

綜上所述,EMILY.RPA系統具備良好的資安防護基礎,整體環境運行穩定且安全可靠。

附件

Sev	CVSS	VPR	EPSS	Name	Family	Count
LOW	2.1 *	3.2	0.3159	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	...	...	...	5 SMB (Multiple Issues)	Windows	6
INFO	...	...	...	2 HTTP (Multiple Issues)	Web Servers	2
INFO				DCE Services Enumeration	Windows	9
INFO				Nessus SYN scanner	Port scanners	4
INFO				Additional DNS Hostnames	General	1
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Device Type	General	1
INFO				Ethernet Card Manufacturer Detection	Misc.	1
INFO				Ethernet MAC Addresses	General	1
INFO				Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO				Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	1

附件

Sev	CVSS	VPR	EPSS	Name	Family	Count
INFO				Nessus Scan Information	Settings	1
INFO				OS Fingerprints Detected	General	1
INFO				OS Identification	General	1
INFO				OS Security Patch Assessment Not Available	Settings	1
INFO				Service Detection	Service detection	1
INFO				Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1
INFO				TCP/IP Timestamps Supported	General	1
INFO				Traceroute Information	General	1
INFO				WS-Management Server Detection	Web Servers	1
INFO				Host Fully Qualified Domain Name (FQDN) Resolution	General	1

THANK YOU

www.dynasafe.com.tw