

IPC 平台 NY 系列中的越界讀取漏洞

發布日期：2025 年 11 月 17 日

台灣歐姆龍股份有限公司

■ 概述

工業用電腦平台 NY 系列的 TPM 2.0 中存在越界讀取 (CWE-125) 漏洞。攻擊者可能利用此漏洞讀取機密資訊，或導致系統當機。

以下列出受此漏洞影響的產品、版本以及減輕風險的對策與迴避方法。透過執行我們建議的對策與迴避方法，可以將此漏洞被利用的風險降至最低。此外，為了讓客戶更加安心地使用產品，我們已準備了針對本次安全性強化的對策版本。關於各產品的對應版本，請參考本文中的對策方法，並請配合實施相關對策。

■ 受影響產品

受影響產品型號及其版本如下所示。

工業用電腦平台 NY 系列

型號	TPM 版本	Lot number (生產日期)
NYB27-□□□□□	5.63 以前	23X25 (2025 年 10 月 23 日)以前
NYB35-□□□□□		
NYB2C-□□□□□		
NYB2A-□□□□□		
NYB55-□□□□□	7.85 以前	
NYB65-□□□□□		
NYB13-□□□□□		
NYB37-□□□□□		
NYB3A-□□□□□		
NYB2E-□□□□□		
NYP27-□□□□□	5.63 以前	
NYP35-□□□□□		
NYP2C-□□□□□		
NYP2A-□□□□□		
NYP55-□□□□□	7.85 以前	
NYP65-□□□□□		
NYP13-□□□□□		
NYP37-□□□□□		
NYP3A-□□□□□		
NYE2A-□□□□□	5.63 以前	

請參考「附件：TPM 版本確認方法」，以了解如何在 NY 系列中確認 TPM 的版本。

有關批號 (Lot No.) 的確認方式說明，請參閱操作手冊中的「ID Information Indication」。

- NYB Industrial Box PC Hardware User' s Manual (W553)
- NYP Industrial Panel PC Hardware User' s Manual (W555)
- NYE Industrial Panel PC Hardware User' s Manual (W634)

■ 說明

在 Trusted Computing Group 發布的 TPM 2.0 參考實作程式 (版本 Rev 1.83、1.59、1.38) 中發現存在越界讀取漏洞 (CWE-125)，可能導致 TPM 資訊外洩或造成服務阻斷 (DoS)。

此漏洞會影響工業用電腦的 Trusted Platform Module (TPM)。任何由 TPM 保護的資料(包含透過 BitLocker 保護的資料)都有可能受到影響。

另外，在 NYB/NYP/NYE 系列工業用電腦中，未使用 TPM 安全功能的使用者不會受到此問題的影響。

■ CWE、CVE、CVSS 評分

越界讀取 (CWE-125)

CVE-2025-2884

CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:H 基本值 6.6

■ 對策

可以透過將產品更新到對策版本來解決此漏洞。

各產品的對策版本及其發佈時間如下所示。

工業用電腦平台 NY 系列

型號	TPM 版本	Lot number (生產日期)	對策版本提供時間
NYB27-□□□□□	5.63 以前	24X25 以降	2025年10月24日
NYB35-□□□□□			
NYB2C-□□□□□			
NYB2A-□□□□□			
NYB55-□□□□□	7.85 以前		
NYB65-□□□□□			
NYB13-□□□□□			
NYB37-□□□□□			
NYB3A-□□□□□			
NYB2E-□□□□□			
NYP27-□□□□□	5.63 以前		
NYP35-□□□□□			
NYP2C-□□□□□			
NYP2A-□□□□□			
NYP55-□□□□□	7.85 以前		
NYP65-□□□□□			
NYP13-□□□□□			
NYP37-□□□□□			
NYP3A-□□□□□			
NYE2A-□□□□□	5.63 以前		

補釘影像發布日期：2025 年 11 月 4 日

注意：若 TPM 更新失敗，工業用電腦（IPC）可能無法啟動。
僅在你能接受此風險的情況下，請執行以下步驟。

TPM 更新步驟

1. 訪問歐姆龍下載頁面：
<https://www.fa.omron.co.jp/member/product/tool/ipcplatform/index.htm>
2. 閱讀頁面下方的軟體使用許可契約，然後點選「同意條款並打開下載頁面」以取得最新版本。
3. 從 [Trusted Platform Module Firmware] 下載對應您使用的 IPC 型號的映像檔。下載後，確認映像檔的 SHA256 雜湊值與下載頁面上提供的值一致。
4. 使用 Rufus [<https://rufus.ie/en/>]，將下載的映像檔製作成可開機的 USB 隨身碟。
5. 反覆按 [DEL] 鍵，將 IPC 啟動至 BIOS。
6. 選擇 [Advanced] → [Trusted Computing]。
7. 選擇 [Security Device Support]，將其設定為 [Disable]。
8. 儲存更改 (F10) 並重新啟動。
9. 連接用於 UEFI Shell 的 USB 隨身碟。
10. 重新啟動 IPC，從 USB 隨身碟啟動。
11. TPM 更新腳本會自動執行，請等待完成。
12. 更新完成後，重新啟動 IPC 並進入 BIOS。
13. 選擇 [Advanced] → [Trusted Computing] → [Security Device Support]，將其改回 [Enable]。

■ 緩解措施和保護方法

為了將這些風險降至最低，歐姆龍建議客戶採取下列緩解措施。

1. 防毒保護

為保護任何可以存取控制系統的 PC 免受惡意軟體的侵害，請確保安裝和維護最新的商業級防毒軟體。

2. 防止未授權存取

- 盡量減少控制系統和設備連接開放網路，以防不信任裝置登入。
- 使用防火牆（關閉未使用的通訊埠，限制通訊主機），將其與 IT 網路隔離。
- 使用虛擬專用網路（VPN）進行遠端連接控制系統及設備。
- 使用高強度密碼並增加修改頻率。
- 安裝實物控制，確保僅授權人員可連結控制系統和設備。
- 在將任何 USB 隨身碟或類似裝置連接到系統和裝置之前，請先掃描病毒以確保其安全。
- 強化對遠端連接控制系統和設備的多重身分驗證。

3. 資料輸入和輸出保護

利用備份和範圍檢查等驗證處理措施，以防控制系統和設備輸入/輸出數據被修改。

4. 資料復原

定期進行數據備份和維護，以防數據丟失。

■ 諮詢方式

如您在採取減輕措施/解決方案時遇到問題，可以透過以下方式聯繫歐姆龍營業據點或經銷商：

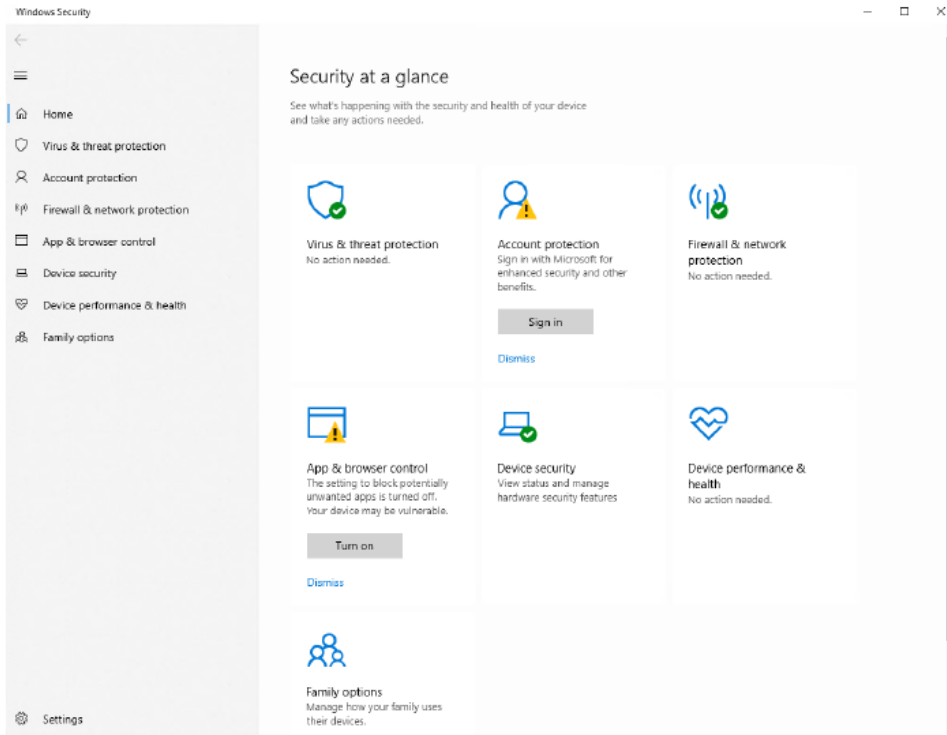
https://www.ia.omron.com/global_network/index.html

■ 更新紀錄

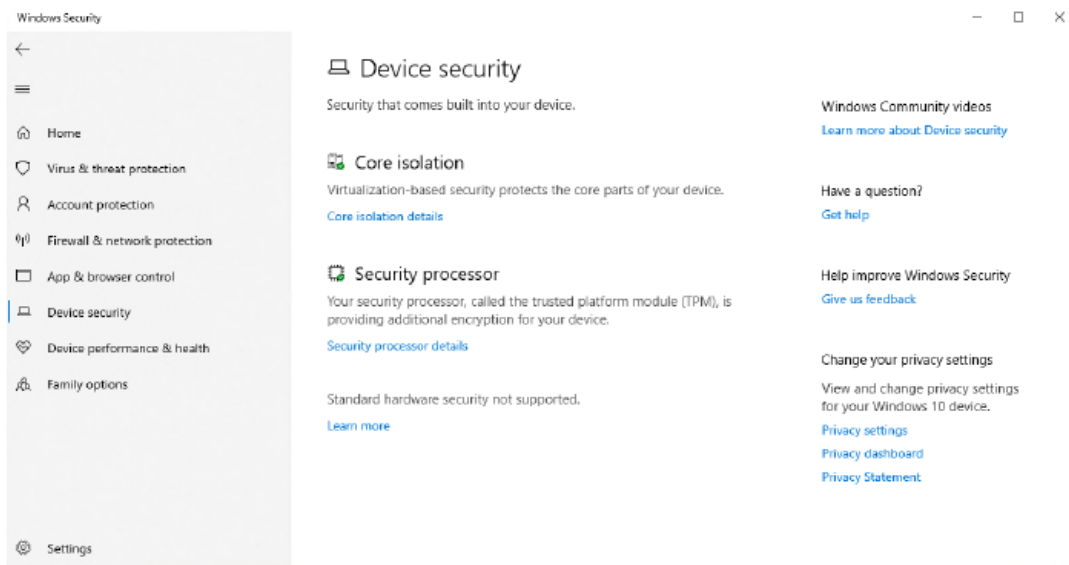
-2025 年 11 月 17 日 發布

附錄—TPM 版本的確認方法

1. 在 Windows 中，開啟 [Windows 安全性]。
將會顯示 Windows 安全性資訊。



2. 選擇 裝置安全性 (Device security)。
將會顯示裝置安全性資訊。



3. 選擇 安全處理器 (Security processor details)。

將會顯示安全處理器的詳細資訊，其中包括 TPM 的製造商版本。

