# 行政院國家資通安全會報技術服務中心

# 漏洞/資安訊息警訊

| | | | |
|---|---|---|---|
| 發布編號 | NCCST-ANA-2017-0014 | 發布時間 | Thu Feb 16 10:10:15 CST 2017 |
| 事件類型 | 攻擊活動預警 | 發現時間 | Thu Feb 16 00:00:00 CST 2017 |
| 警訊名稱 | 工業與環境控制設備無身份驗證機制或使用預設密碼，並曝露於網際網路上，恐有資訊外洩與遭受入侵之疑慮 | | |
| 內容說明 | 本中心近期執行僵屍網路調查案時，發現有特定 IP 對工業控制與環境控制設備進行掃描，且確認部份機關所使用的環境控制設備已曝露在網際網路上，並且未設定密碼或使用預設帳號密碼等情況，可能有資訊外洩與遭受駭客入侵之疑慮。<br><br>由於相關控制設備可被使用於環境控制、工業控制及交通號誌等系統，主要作為電力、水力、溫度及消防等訊號轉換控制之使用，請各機關盤點與檢視是否使用相關設備，對該設備加強權限控管並避免使用公開的網際網路位置，以及加強防範措施。<br><br>若發現設備遭到入侵，請立即進行通報應變處置。 | | |
| 影響平台 | 多款環境與工業控制設備 | | |
| 影響等級 | 中 | | |
| 建議措施 | 1.盤點與檢視是否使用環境控制、工業控制及交通號誌等相關裝置。<br><br>2.裝置上所有帳號需設定強健的密碼，非必要使用的帳號請將其刪除或停用。系統上非必要的服務程式亦建議移除或關閉。<br><br>3.建議裝置設備不要使用公開的網際網路位置，如無法避免使用公開的網際網路位置，建議裝置設備前端需有防火牆防護，並採用白名單方式進行存取過濾。<br><br>4.檢驗防火牆規則，確認個別系統僅開放所需對外提供服務之通訊埠。<br><br>5.若無防火牆可考慮安裝防火牆或於 Windows 平台使用 Windows XP/7/8/2008 內建之 Internet Firewall/Windows Firewall 或 Windows 2000 之 TCP/IP 篩選功能。Linux 平台可考慮使用 iptables 等內建防火牆。 | | |

| | |
|---|---|
| | 6.建議將控制設備更新韌體至最新版本。 |
| 參考資料 | 無 |

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw