利凌企業股份有限公司網路商品資安漏洞修正通知

文件編號: M00166
日期: 03/02/2021
部門: 技術支援部

說明
利凌近日發現本公司生產 P2/Z2/P3/Z3 攝影機系列商品，有資安漏洞疑慮，若您的 P2/Z2/P3/Z3 攝影機有，下列情事，請立即更新韌體。

(1) 使用預設密碼
(2) 使用 Internet IP 位址存取設備

若您使用 NVR P2P 進行 Internet 連線方式，而攝影機採 LAN 連線模式，則無上述資安疑慮。
若您使用 VPN 進行 Internet 連線方式，則無上述資安疑慮。

受影響相關產品型號:

P2/Z2: Firmware 7.1.94.8908 或更低版本有資安疑慮。
P3/Z3: Firmware 8.1.94.8908 或更低版本有資安疑慮。

韌體修訂版本
For P2/Z2 系列 7.1.94 SVN 9764
https://www.dropbox.com/s/8w6psgsgcaxbk2j/flashS3LM.bin?dl=0

For P3/Z3 系列 8.1.94 SVN 9737 韌體版本
https://www.meritlilin.com/index.php/en/support/file/type/Firmware

資安漏洞說明
- NTP 設定頁面存在命令注入弱點
- 裝置設定頁面 (路徑: Advance >> System >> Timer) 提供使用者設定, 校時伺服器 (NTP Server)，除了預設選項外亦提供使用者自行定義(User defined) Time Server
- /new/create.htm 與 /apply2.cgi 存在權限跨越弱點
- /new/setup.htm 洩漏 admin 帳號密碼

處理建議
1. 立即進行網路韌體更新。
2. 更改使用者名稱及密碼。
3. 更改通信埠 port 號。

其他資源
- 利凌網路產品資安策略及漏洞公告請參閱此連結。
- 回報網路資安議題，請洽 security@meritlilin.com.tw。

本案由 TWCERT/CC （台灣電腦網路危機處理暨協調中心）於 2021 年 1 月 25 日通報本公司，本公司於 2021 年 2 月 2 日回覆 TWCERT/CC。

聯絡方式
請聯絡利凌全球經銷商，或登錄 ZenDesk 獲得更多訊息及問題回報。