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: M00163
日期: 10/22/2020
部門: 技術支援部

說明
利凌近日發現本公司生產 DVR/NVR 系列商品，有資安漏洞疑慮，若您的 DVR/NVR 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 P2P 進行 Internet 連線方式，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。

相關產品型號:
DH032: Firmware v1.0.28.3858 或更低版本
DVR708, DVR716, DVR816: Firmware v1.3.4 或更低版本
NVR100L, NVR200L, NVR400L, NVR1400L, NVR2400L: Firmware v1.1.66 或更低版本
NVR3216, NVR3416, NVR3416r, NVR3816: Firmware v2.0.74.3921 或更低版本
NVR5832, NVR5832S: Firmware v4.0.24.4043 或更低版本
NVR5104E, NVR5208E, NVR5416E: Firmware v4.0.24.4078 或更低版本

韌體修訂版本: 可於此處下載或公司官網.

資安漏洞
/getclock CGI 指令使用預設密碼，開啟 NTP 主機進行通信並有可能被植入 DDoS 攻擊。

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 360 的安全研究員馬延龍（mayanlong@360.cn）和葉根深（yegenshen@360.cn）回報本公司該漏洞。本公司於 9/25/2020 收到弱點通知並於 9/26/2020 修復並回報。

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。