02/27/2020

敬愛的利凌客戶:

感謝使用利凌企業相關網路產品。近日被揭露利凌銷售的相關 DVR 商品資安漏洞,本公司針對此事件評估其風險為 CVSS v3.1 Base Score of 10.0 (最高風險) ,並建議客戶立即進行 DVR 韌體更新。

利凌此次為改善產品資安漏洞事件,已有對應政策並提供相應韌體改善資安漏洞。

受影響之產品線
DHD5、DHD3 和 DHD2 系列,共計有三個產品系列使用相同的韌體架構。

受影響之產品型號與影響數量
受影響產品型號:DHD516A、DHD508A、DHD504A、DHD316A、DHD308A、DHD304A、DHD204、DHD204A、DHD208、DHD208A、DHD216、DHD216A。

預估影響全球 13,062 台 DVR。

不受影響之產品線
新發布的 DVR 產品線 DHD5104、DHD5216 和 DHD5108 不在此次事件影響內。

利凌全系列 IP 攝影機產品與全系列 NVR/Decoder 解碼器/VMS 產品,不在此次事件影響內。

此次資安事件的攻擊手段
使用登入 DVR 系統的預設帳號,並採用注入腳本代碼的方式來攻擊其他 Internet 設備。

1. 將透過 DVR 使用 DDoS 攻擊其他網際網路設備。
2. 透過腳本代碼執行系統命令。
3. 連線方式將會由 PPPoE 更改為 DHCP。
4. 透過 NTP、FTP 注入腳本代碼的方式來執行攻擊。

韌體更新事項
1. 韌體升級後,第一次登入系統時,將強制用戶需變更預設的帳號和密碼。
2. 將驗證 NTP 服務器和 FTP 服務的主機名稱及其內容,以防止注入腳本代碼。
3. 增加系統加密機制,以防止注入與執行任何 Linux 腳本或命令。

利凌目前已執行的行動
1. 在利凌官方網站上公告此次資安事件,並提供更新之韌體。
2. 利凌在資安弱點網站中公告此次產品資安事件,並通報受影響之產品。
3. 透過利凌 ERP 和 MES 系統,查詢 DVR 所銷售的地區與客戶。
4. 透過利凌業務單位與分公司告知全球經銷商和系統整合商進行韌體更新。

事件通報時間序
2020 年 2 月 10 日:奇虎 360 技術有限公司將所發現的漏洞通知利凌。
2020 年 2 月 10 日:利凌回覆奇虎 360 並詢問產品型號及漏洞問題。
2020 年 2 月 12 日:利凌證實了該資安問題,並向奇虎回覆已進行了韌體修復。
2020 年 2 月 14 日:利凌在資安弱點網站上發布了此次資安事件與解決方案。

利凌其他資訊安全改進說明
首先，針對此次利凌資安事件造成不便之處,敬請見諒。

為了加強網路產品的資安要求,利凌於 2019 年開始透過台灣資通產業標準協會 (TAICS) 所立之資安標準 TAICS TS-0014-2 v2.0 ,送驗網路產品的相關認證。

基於 TAICS TS-0014-3 標準,利凌已於 2020 年初針對 NVR / DVR 系列進行認證。

利凌聘請第三方單位檢測單位,台灣 Deloitte (勤業眾信聯合會計師事務所)及 ETC (台灣電子測試中心), 根據 TAICS 的規範進行資安檢查。

目前利凌 NVR 5 系列產品,已於 2020 年 2 月開始遵循美國加州物聯網安全法規範。

利凌 DHD5104、DHD5216 和 DHD5108 系列產品,已使用加密韌體技術預防攻擊者進行反組譯分析。

目前利凌 IP 攝影機 P2、Z2、P3、Z3、P5、Z5、M、S 與 Ultra 系列,已於 2020 年 2 月開始遵循美國加州物聯網安全法規範。

利凌 NVR 3 系列及 5 系列 將於 2020 年第二季導入加密的韌體來預防攻擊者進行韌體反組譯分析。

利凌已於 2020 年 2 月開始提供 RTSP over HTTPs 影像串流加密技術於,利凌 IP 攝影機和利凌 NVR /混合型 DVR 連線使用。

最後、我們為此次事件造成客戶的不便深感抱歉。利凌秉持 40 年的服務理念,持續加強網路產品的資安要求。

如有任何疑問,請隨時與我們全球業務人員聯絡。

產品管理部
利凌企業股份有限公司