

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	ICST-ANA-2013-0018	發布時間	Tue Aug 06 17:16:06 CST 2013
事件類型	攻擊活動預警	發現時間	Tue Aug 06 00:00:00 CST 2013
警訊名稱	播放軟體 KMPlayer 更新機制異常，請各單位注意並提高警覺		
內容說明	<p>技服中心接獲外部情資，播放軟體 KMPlayer 更新機制異常，駭客疑似透過播放軟體 KMPlayer 更新機制散播惡意程式。</p> <p>KMPlayer 執行後，若出現版本 3.7.0.87 更新訊息，將連線至 http://cdn.kmplayer.com/player/update 下載偽冒更新程式(KMP 3.7.0.87.exe)。</p> <p>偽冒更新程式執行後，並不會變更原 KMPlayer 版本，但將植入惡意程式於下述資料夾(預設隱藏)：</p> <p><u>Windows XP</u></p> <p>C:\Documents and Settings\All Users\OleView\ACLUI.DLL C:\Documents and Settings\All Users\OleView\ACLUI.DLL.UI C:\Documents and Settings\All Users\OleView\OleView.exe</p> <p><u>Windows 7</u></p> <p>C:\ProgramData\OleView\ACLUI.DLL C:\ProgramData\OleView\ACLUI.DLL.UI C:\ProgramData\OleView\OleView.exe</p> <p>目前已知受感染電腦會連線以下中繼站:</p> <p>-pen.abacocafe.com -pens.abacocafe.com -cdn.abacocafe.com -vpen.abacocafe.com</p> <p>KMPlayer 源自韓國的一套播放軟體，最新版本為 3.6.0.87，支援各種常見的影音檔播放，且內建多國語系，由於使用情況相當普遍，影響範圍與衝擊不容小覷。請各機關立即清查機關內是否有連線上述中繼站的行為，若發現中繼站連線或異常行為，請立即至通報應變網站(https://info.cert.tane.edu.tw/) 進行資安事故通報。</p>		
影響平台	所有 KMPlayer		
影響等級	高		

建議措施	<p>1.若發現上述惡意程式，請盡速刪除，或可透過下述防毒軟體進行偵測：</p> <p>(1)OfficeScan(趨勢科技) 病毒碼版次：CPR 10.200.01</p> <p>(2)SmartScan(趨勢科技) 病毒碼版次：TBL 13436.002.00</p> <p>(3)Avira 病毒碼版次：7.11.94.64</p> <p>2.更新播放軟體 KMPlayer 時，注意更新版次是否與官網相符(目前官方最新版本為 3.6.0.87)。</p> <p>3.此攻擊事故已通知韓國相關單位，目前尚未接獲進一步處理說明，建議暫時停用多媒體播放軟體 KMPlayer，改用其他播放軟體。</p>
參考資料	無