駭客假冒行政院國家資安會名義發送惡意電子郵件威脅公告

主旨：

請加強防範駭客偽冒行政院國家資通安全會報名義發送之惡意電子郵件

威脅說明：

教育部技服中心近日接獲關貿網路股份有限公司情資，發現駭客利用漏洞 CVE-2014-4114 偽冒行政院國家資通安全會報(名稱顯示為 NICST.EY)名義散播 APT 郵件。

該郵件附檔為「雲端資安.ppsx」，使用者若開啟檔案將被自動植入並執行惡意程式 slide2.gif 於%TEMP%路徑之下，並連線至惡意程式下載點 70.88.151.213 (下載並執行 tmp.exe，驗證時已無法存取)，成功的攻擊可能使駭客遠端執行任意程式碼，導致使用者資訊遭竊。

請留意勿開啟不明來源或偽冒來源之郵件附檔，以降低遭受攻擊風險。

影響等級：

中。

影響平台：

N/A。

建議措施：

1.請留意勿開啟不明來源或偽冒來源之郵件附檔。

2.安裝 MS14-060 更新 (但此更新修補尚不完整，已安裝 patch 的情況下打開該投影片會跳出是否執行 slide2.inf 的詢問視窗)

參考資料：

https://technet.microsoft.com/zh-tw/library/security/ms14-060.aspx

http://www.isightpartners.com/2014/10/cve-2014-4114/#sthash.vYsbO6oC.dpuf

3.監控或阻擋此惡意程式之下載點(70.88.151.213)