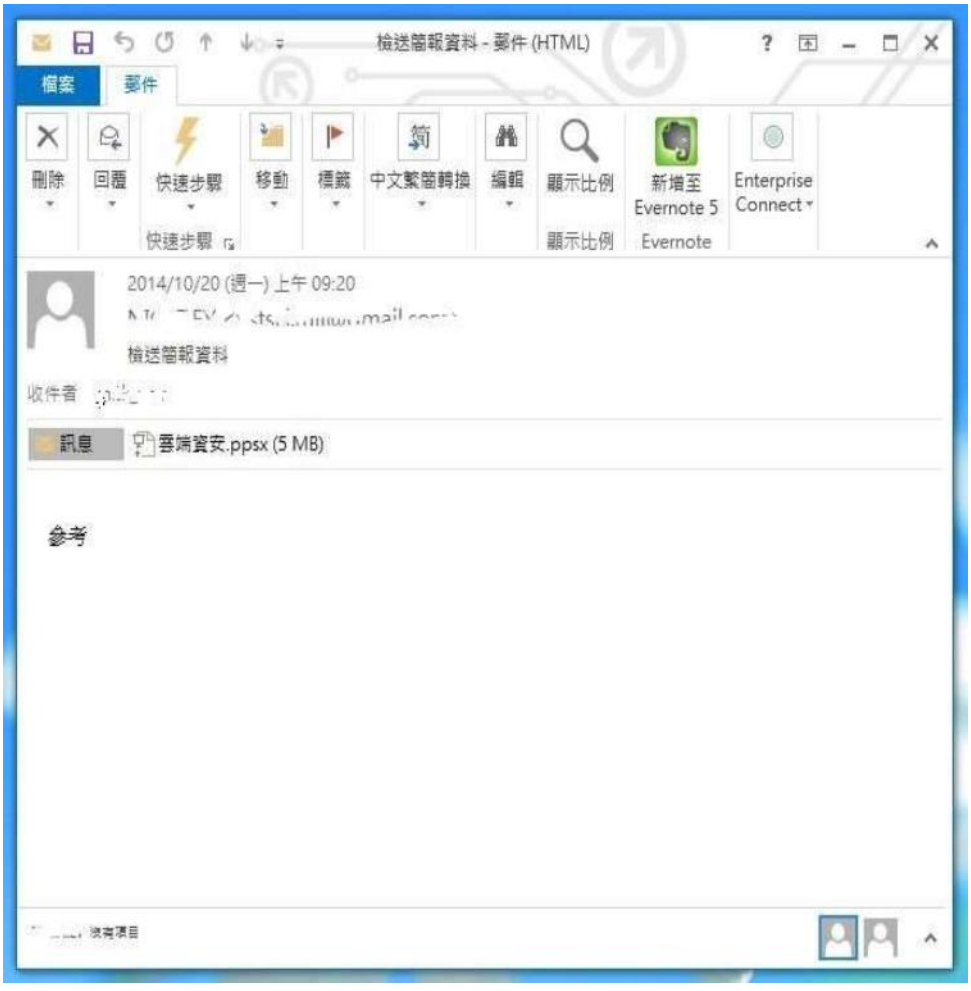
微軟作業系統零時差弱點 CVE-2014-4114 威脅說明

(一) 威脅說明：

微軟才在上週二發布的例行性安全公告，其中新發現的零時差漏洞 CVE-2014-4114，之前傳出有駭客透過此漏洞成功竊取北大西洋公約組織與歐盟等企業的重要資料，**目前已在台灣發現駭客透過此漏洞攻擊的蹤影。**

一封名為「檢送簡報資料」的郵件，其中包含了一個名為「雲端資安.ppsx」的附件檔(如下圖)。若不慎開啟，內嵌在文件裡的 PE 病毒將被自動執行。造成使用者電腦暴於資料被竊的風險中。



病毒程式如下圖：

(二) 影響等級：

高。

(三) 影響平台：

此漏洞影響 Vista 之後所有版本的 Windows 作業系統 與 Windows Server 2008 及 2012。

(四) 建議措施：

趨勢科技的 APT 防護解決方案已可針對此漏洞進行防護，透過” 惡意文件指紋偵測引擎” (ATSE 靜態引擎)成功偵測並攔阻此社交工程之惡意文件。

趨勢科技用戶請更新最新防毒元件，以偵測此病毒程式。若有使用 TrendMicro Deep Security 與 OfficeScan IDF plug-in 的用戶們亦可套用下方 DPI 規則進行偵測。

- 1006290 – Microsoft Windows OLE Remote Code Execution Vulnerability (CVE-2014-4114)
- 1006291 Microsoft Windows OLE Remote Code Execution Vulnerability (CVE-2014-4114) – 1

此外，我們建議用戶盡快針對此一 Windows 作業系統的漏洞進行修補，在完成修補前，**不要隨意開啟陌生人寄來的 PowerPoint 檔案**，以降低被攻擊的風險。

詳細的攻擊資訊及手法可參考下列 URL：

- http://blog.trendmicro.com/trendlabs-security-intelligence/an-analysis-of-windows-zero-day-vulnerability-cve-2014-4114-aka-sandworm/

- http://blog.trendmicro.com.tw/?p=10171