事件通告：(弱點編號 CVE-2014-1770) IE 8 存在允許遠端執行任意程式碼的 Zero-Day 弱點，請升級 IE 版本或調整設定！

2014/05/23

風險等級：警戒狀態

摘　　要：【弱點說明】

Microsoft Internet Explorer 存在允許遠端執行任意程式碼的 Zero-Day 弱點(弱點編號 CVE-2014-1770) ，惡意人士可透過引誘使用者瀏覽事先建立的惡意網頁後，便可執行任意程式碼、提升權限、規避部份安全限制等讓使用者系統受駭之安全性弱點。目前已知會受到影響的版本為 Internet Explorer 8 版本，中華電信 SOC 建議請使用者升級 IE 版本或調整設定。

【細節描述】

Microsoft Internet Explorer 8 存在允許遠端執行任意程式碼的弱點，此為 Internet Explorer 針對 CMarkup::CreateInitialMarkup 程序無法處理使用釋放後記憶體錯誤(use-after-free) ，可被惡意人士利用並製作有弱點的網頁誘騙受害者連線，誘騙成功後即可取得受害電腦之系統管理者權限。

惡意人士可透過引誘使用者瀏覽事先建立的惡意網頁後，便可執行任意程式碼、洩露機敏性資訊、規避部份安全限制。中華電信 SOC 在此建議請使用者升級 IE 版本或調整設定，並勿隨意瀏覽來源不明的網頁以及開啟郵件附加檔案，以降低受駭風險。

【影響範圍】

Internet Explorer 8 版本。

【建議措施】

(1) 請升級 IE 版本至最新版本 (XP 無法更新至 IE 8)。
(2) 請關閉 ActiveX 及 Active Scripting 功能。
(3) 微軟已釋出 EMET 工具，請使用該工具進行防護 (XP 無法適用此防護手段)。

【參考資料】

- US-CERT

- CVE-2014-1770
- TippingPoint

本資訊轉自教育部資安服務網