微軟 Windows JScript 元件遭爆有零時差漏洞

JScript 處理錯誤物件時，於腳本採取行動時，駭客可以讓一個指標在釋放後重新被使用，再藉由該漏洞執行程式。目前微軟尚未釋出修補程式。

文/陳曉莉 | 2018-05-31 發表

趨勢科技旗下的零時差倡議（Zero-Day Initiative，ZDI）專案本周揭露微軟 Windows 作業系統中的 JScript 元件含有一零時差漏洞，將允許駭客自遠端執行任意程式。

JScript 與 JavaScript 是同樣的程式語言，為了避免商標爭議，微軟於 Windows 中將它稱為 JScript。

ZDI 表示，此一漏洞存在於 JScript 處理錯誤物件，於腳本中採取行動時，駭客可以讓一個指標在釋放後重新被使用，再藉由該漏洞執行程式。這是一個需要使用者互動的漏洞，當駭客誘導使用者開啟一個惡意檔案或造訪惡意網頁時即可開採該漏洞。

ZDI 早在今年 1 月 23 日就向微軟提報該漏洞，但微軟在 120 天的限期內都未修補，使得 ZDI 只好在沒有修補程式的狀態下公開該漏洞。ZDI 並未公布漏洞細節，僅說目前唯一緩解之道是只與可靠的檔案互動。

資料來源：iThome