行政院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	NCCST-ANA-2019-0120	發布時間	Thu Sep 26 08:51:57 CST 2019
事件類型	漏洞預警	發現時間	Tue Sep 24 00:00:00 CST 2019
警訊名稱	微軟 Internet Explorer 與 Windows Defender 存在安全漏洞(CVE-2019-1367 與 CVE-2019-1255)，允許攻擊者遠端執行任意程式碼與阻斷服務，請儘速確認並進行更新		
內容說明	研究人員發現，微軟 Internet Explorer 腳本引擎處理記憶體物件過程中，會造成記憶體毀損，導致攻擊者可利用此漏洞，進而遠端執行任意程式碼(漏洞編號為 CVE-2019-1367)，且此漏洞已有攻擊程式，應儘速修補。 另微軟 Windows Defender 惡意程式防護引擎(Malware Protection Engine)處理檔案不當，導致攻擊者可利用此漏洞執行阻斷服務攻擊(漏洞編號為 CVE-2019-1255)。		
影響平台	1.CVE-2019-1367：Internet Explorer 9、10 及 11 版本 2.CVE-2019-1255： (1)Microsoft Windows 7、8.1、10、Server 2008、Server 2012、Server 2016、Server 2019 的 Windows Defender (2)Microsoft System Center Endpoint Protection、Microsoft Forefront Endpoint Protection 2010、Microsoft System Center 2012 Endpoint Protection、Microsoft System Center 2012 R2 Endpoint Protection (3)Microsoft Security Essentials		
影響等級	高		
建議措施	目前微軟官方已針對弱點釋出修復版本，網址如下，請儘速進行更新： 1. https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1367 2. https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1255		

參考資料	1. https://www.hkcert.org/my_url/zh/alert/19092401 2. https://www.ithome.com.tw/news/133226 3. https://www.zdnet.com/article/microsoft-releases-out-of-band-security-update-to-fix-ie-zero-day-defender-bug/#ftag=RSSbaffb68

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw