張貼日期：2017/04/06

[資安漏洞預警公告] Microsoft Windows Server 2003 IIS的WebDAV服務存在緩衝區溢位弱點

主旨：Microsoft Windows Server 2003 IIS的WebDAV服務存在緩衝區溢位弱點，允許攻擊者遠端執行任意程式碼或造成阻斷服務。

說明：

1. 該漏洞主要是Microsoft IIS(Internet Information Services)6.0的WebDAV服務中，httpext.dll動態連結函式庫之ScStorageFromUrl函式存在緩衝區溢位漏洞，讓遠端攻擊者可透過發送特製的的PROPFIND請求封包，導致可執行任意程式碼或造成阻斷服務。
2. WebDAV(Web-Based Distributed Authoring and Versioning)是一種可與遠端主機進行檔案或資料交換的標準，擁有權限的使用者可透過網路存取遠端目標網站的WebDAV資料夾內的檔案。
3. 影響平臺：Microsoft Windows Server 2003的IIS 6.0
4. 建議措施:
    1. 請確認是否使用Microsoft Windows Server 2003的IIS 6.0，並啟用WebDAV服務(可至Application Server→Internet Information Services→World Wide Web Service→WebDAV Publishing檢視是否有勾選啟用，預設是未啟用該服務)。
    2. 如仍須使用WebDAV服務，建議將作業系統與IIS升級至最新的版本。
    3. 其餘未在上述受影響之作業系統的IIS 6.0，仍請密切注意微軟官方(https://technet.microsoft.com/en-us/security/bulletins.aspx)是否有後續消息。
5. 參考資料:
    1. https://nvd.nist.gov/vuln/detail/CVE-2017-7269
    2. http://www.ithome.com.tw/news/113166
    3. https://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/3cbec1c7-e3ed-43d3-86e8-ce94e4375e70.mspx?mfr=true

---

計算機與通訊中心
網路系統組 敬啟