一、弱點知識庫

＊WordPress 釋出 4.5.2 版安全更新

說明	WordPress 存在弱點，在多媒體撥放器的第三方 JavaScript 庫中的 MediaElement.js 有 XSS 的弱點。此漏洞可被利用於使用特定的 URL 執行跨站指令碼（Cross-site Scripting，XSS）攻擊。
影響	遠端攻擊者可能藉此漏洞取得網頁控制權
影響系統	-WordPress 4.5.1 (含)之前版本
建議解決方法	1. 建議使用者應儘速將目前使用版本更新至最新之版本。 2. 相關網站： https://wordpress.org/news/2016/05/wordpress-4-5-2/

＊VMware 存在多個弱點，攻擊者可利用此弱點並執行任意程式碼

說明	遠端攻擊者可能利用 Oracle 的 JRE RMI 伺服器的 JMX 反序列化身份驗證弱點，編號為 CVE-2016-3427 與 CVE-2016-2077 的弱點，允許遠端攻擊登入主機執行任意程式碼。
影響	遠端攻擊者可利用此弱點，執行任意程式碼。
影響系統	-vCenter Server 6.0 on Windows without workaround of KB 2145343 -vCenter Server 6.0 on Linux (VCSA) prior to 6.0.0b -vCenter Server 5.5 prior to 5.5 U3d (on Windows), 5.5 U3 (VCSA) -vCenter Server 5.1 prior to 5.1 U3b -vCenter Server 5.0 prior to 5.0 U3e -vCloud Director prior to 8.0.1.1 -vCloud Director prior to 5.6.5.1 -vCloud Director prior to 5.5.6.1 -vSphere Replication prior to 6.1.1 -vSphere Replication prior to 6.0.0.3 -vSphere Replication prior to 5.8.1.2 -vSphere Replication prior to 5.6.0.6 -vRealize Operations Manager 6.x (non-appliance version) -vRealize Infrastructure Navigator prior to 5.8.6 -VMware Workstation prior to 11.1.3 -VMware Player prior to 7.1.3
建議解決方法	1. 建議使用者應儘速將目前使用版本更新至最新之版本。 2. 相關網站： http://www.vmware.com/security/advisories/VMSA-2016-0005.html http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3427 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2077

二、惡意程式分析報告

(一)前言

誘捕網路（Honeynet）即是一個可以誘捕駭客活動與行為、收集各項威脅的方式的網路。Honeynet是一種屬於高互動式的誘捕系統群，主要是由多個有缺陷、不具營運價值的誘捕系統(Honeypot)所構成，藉由模擬真實的系統行為和網路服務回應，不僅可以誘使駭客進行攻擊，還可捕捉並紀錄攻擊手法和系統行為的改變，並將蒐集到的攻擊資訊回饋給相關人員進行分析並改善網路防禦的方法。

本分析報告即是針對『教育部教育學術資訊安全監控中心(A-SOC)暨殭屍電腦(Botnet)防禦機制建置計畫』所佈署之Honeynet誘捕網路所蒐集到之惡意程式進行分析說明。

(二)惡意程式分析

(1) 惡意程式基本資料

- 單一識別碼(Hash 值)
  - MD5：c01f3904814b5ee1c03c11785df33726
  - SHA-1：35946cfdbef3a0cbc9e9086d8271bf1260588214
- 惡意程式檔案大小： 228,352 bytes
- 各防毒軟體定義名稱：
  - Avira：TR/Ransom.JigsawLocker.bqvf
  - BitDefender：Gen:Variant.Zusy.187295
  - Fortinet：W32/Agent.B!tr
  - Kaspersky：Trojan.Win32.Agent.nevnsw

(2)惡意程式行為分析

- 存取主機資訊，此惡意程式在感染主機後，會試圖存取主機的系統資訊，例如讀取 MachineGuid、DigitalProductid 與 SystemBiosDate。
  - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ComputerName
- 修改啟動清單：該惡意程式在感染主機後，會修改受害電腦的系統啟動清單，藉由偽裝為系統服務，讓受害主機每次都會重新啟動該程式。
  - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- 干擾砂箱分析作業，此惡意程式會透過休眠(Sleep)的指令，在感染受害主機後會靜止 1,566,864 秒(超過 18 天)。
- 該惡意程式會讀取受害主機的瀏覽器歷史紀錄，藉此竊取使用者的網頁瀏覽紀錄。
  - C:\\Documents and Settings\\Default User\\Local Settings\\History\\History.IE5\\index.dat

(3) 提升本機安全性防護

- 安裝防毒軟體並定期更新病毒碼：建議電腦使用者必須要安裝防毒軟體並定期病毒碼，避免網路威脅發生。
- 開啟本機防火牆並定期安裝系統更新：開啟微軟系統內建之系統更新功

能，定期針對系統重大更新以及安全性更新檔進行安裝，避免系統暴露在攻擊的威脅之下。

➢惡意程式移除工具:若使用者的電腦系統不慎遭到此惡意程式感染而無法正常運作，請下載各大防毒軟體廠商所釋出之惡意程式移除工具，以進行病毒清除程序。以下網址可供參考：

- Microsoft Safety Scanner,官方網站：
  http://www.microsoft.com/security/scanner/zh-tw/default.aspx
- TrendMicro System Cleaner,官方網站：
  http://downloadcenter.trendmicro.com/index.php?regs=TW
- Norton Rescue Tool,官方網站：
  http://tw.norton.com/free-tools-trial/promo
- Google Chrome Cleanup Tool, 官方網站：
  https://www.google.com/chrome/cleanup-tool/