一、弱點知識庫

＊Joomla! 3.2 版以上存在 SQL injection 漏洞

說明	Joomla!是一套相當知名的內容管理系統（Content Management System, CMS），內容管理系統是一種用來管理網站上的內容的應用程式，網站上的內容包括文字、照片、影片、音樂、檔案文件等等。CVE-2015-7857 漏洞存在於 Joomla! 3.2 到 3.4.4 版，遠端攻擊者如利用此漏洞成功，可取得管理員權限，進一步控制整個網站並執行其他攻擊。
影響	遠端攻擊者可利用此漏洞，取得網站管理權限。
影響系統	Joomla! 3.2 版本以上皆收影響。
建議解決方法	1.建議使用者應儘速更新至最新版本。 2.相關網站： https://github.com/joomla/joomla-cms/releases/tag/3.4.5 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7857

＊Stagefright 2.0 漏洞

說明	Stagefright 本身並不是一種漏洞，而是 Android 操作系統的核心組成框架之一，主要用來處理、播放和記錄多媒體文件。遠端攻擊者只要利用編號為 CVE-2015-6602 的漏洞，進一步傳遞內含特殊媒體檔案的多媒體簡訊給使用者，不需使用者的互動就能在手機上遠端執行任意程式。
影響	遠端攻擊者可利用此漏洞，執行任意程式。
影響系統	所有 Android 版本。
建議解決方法	1.建議使用者不要點選來路不明的連結。 2.及時更新系統。 3.參考資料： https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6602

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

(1)單一識別碼(Hash值)

◆MD5：a479c0649644742552a08076f682b16d
71c0568c4f6e22baded5d150c2854bff

◆SHA-1：1fac28ec3dec799337e7f43bfbc714640a1c4515

(2)惡意程式檔案大小：89,600 bytes

(3)各防毒軟體定義名稱：

◆ ESET-NOD32：unknown
◆ GData：Macro.Trojan-Downloader.Agent.FV
◆ Kaspersky：unknown
◆ TrendMicro：unknown
◆ McAfee：unknown

2.惡意程式行為分析

(1) 新增檔案

這隻惡意程式會在受害者的系統磁區中新增以下檔案：

◆ C:\Program Files\Common Files\Microsoft Shared\office12\Cultures\office.odf
◆ C:\Documents and Settings\User\Local Settings\Temporary Internet Files\Content.IE5\4XEJWTA3\6h54gf[1].exe

(2)該惡意程式在被執行後，會透過修改以下機碼，將外部主機128.199.122.196以及網域名稱malerkutzner.de加入瀏覽器的信任主機清單中

◆ HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\Domains\128.199.122.196
◆ HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\128.199.122.196
◆ HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\Domains\malerkutzner.de

◆ HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\malerkutzner.de

(3) 資訊蒐集

該惡意程式會蒐集系統資訊，包含系統BIOS時間，MachineGuid...等，並存取本機的瀏覽器瀏覽歷史紀錄，來蒐集被害主機上的網頁瀏覽行為。

(4)與外部主機進行聯絡

該惡意程式在成功感染受害主機後，會從外部主機下載檔案，資訊如下：

◆ 網域名稱：malerkutzner.de

✓ IP：82.165.90.27

✓ 國家：德國

✓ 連線位置：http://malerkutzner.de/00o98k76/6h54gf.exe

◆ IP：128.199.122.196 國家：英國

(三) 提升本機安全性防護

1.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。

2. 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。

3.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：

(1)Microsoft Safety Scanner,官方網站：
http://www.microsoft.com/security/scanner/zh-tw/default.aspx

(2)TrendMicro System Cleaner,官方網站：
http://downloadcenter.trendmicro.com/index.php?regs=TW

(3)Norton Rescue Tool,官方網
http://tw.norton.com/free-tools-trial/promo