

作者:阿龍

Microsoft Baseline Security Analyzer V1.2.1 (微軟系統安全漏洞分析)

一.說明:

近年來隨著 WINDOWS 系統的漏洞不斷的被發現，電腦病毒更加變本加厲的肆虐在每一臺電腦上，加上日益在網絡上流通的駭客工具更是給 WINDOWS 系統造成了巨大的危害。微軟也為此忙的不亦樂乎，不斷的推出新的修補程序和安全加密程序，但是系統管理員未必就完全了解 WINDOWS 2K/XP 是否完全修正了所有的系統漏洞。因此微軟推出了一款名為 Microsoft Baseline Security Analyzer(MBSA),讓系統管理員了解和修正 WINDOWS 2K/XP 的安全漏洞。

二.檢測的漏洞:

[系統]

Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003。

[應用軟體]

Internet Information Server (IIS), SQL Server, Internet Explorer, Office, Exchange Server, Windows Media Player, Microsoft Data Access Components (MDAC), MSXML, Microsoft Virtual Machine, Commerce Server, Content Management Server, BizTalk Server, Host Integration Server。

三.注意事項:

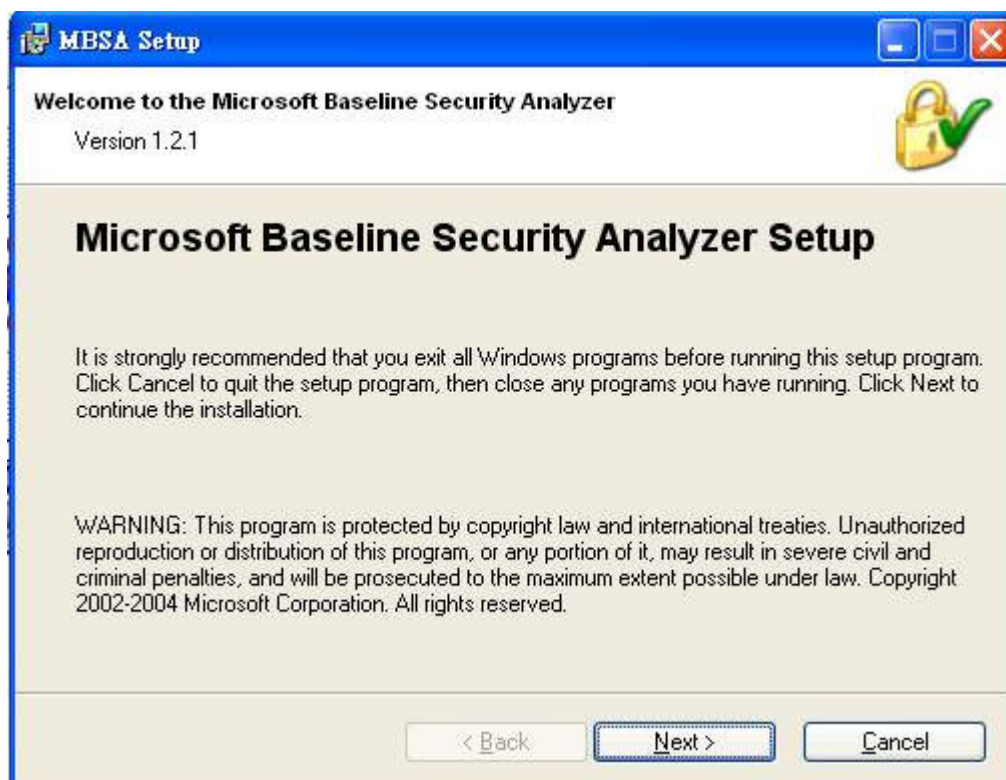
1、MBSA 只支援 WINDOWS NT、WINDOWS 2000、WINDOWS XP 的系統，不支援任何 WINDOWS 9X 的系統進行安全漏洞檢測。

2、根據 MBSA 的安全漏洞報告內的"How to correct this"，進入專門連接的 Windows Update 網頁進行相關的程序修補，但並不會把漏洞報告裏所出現的問題全部修補完，系統管理員需要重新在 MBSA 的漏洞報告裏逐個把漏洞修補完全。完全修正好後，重新啓動電腦即完成漏洞的修補。

MBSA 下載位置:

<http://download.microsoft.com/download/9/0/7/90769f0c-c025-48bf-a9c7-60072d0cb717/MBSASetup-EN.msi>

四.MBSA 安裝:



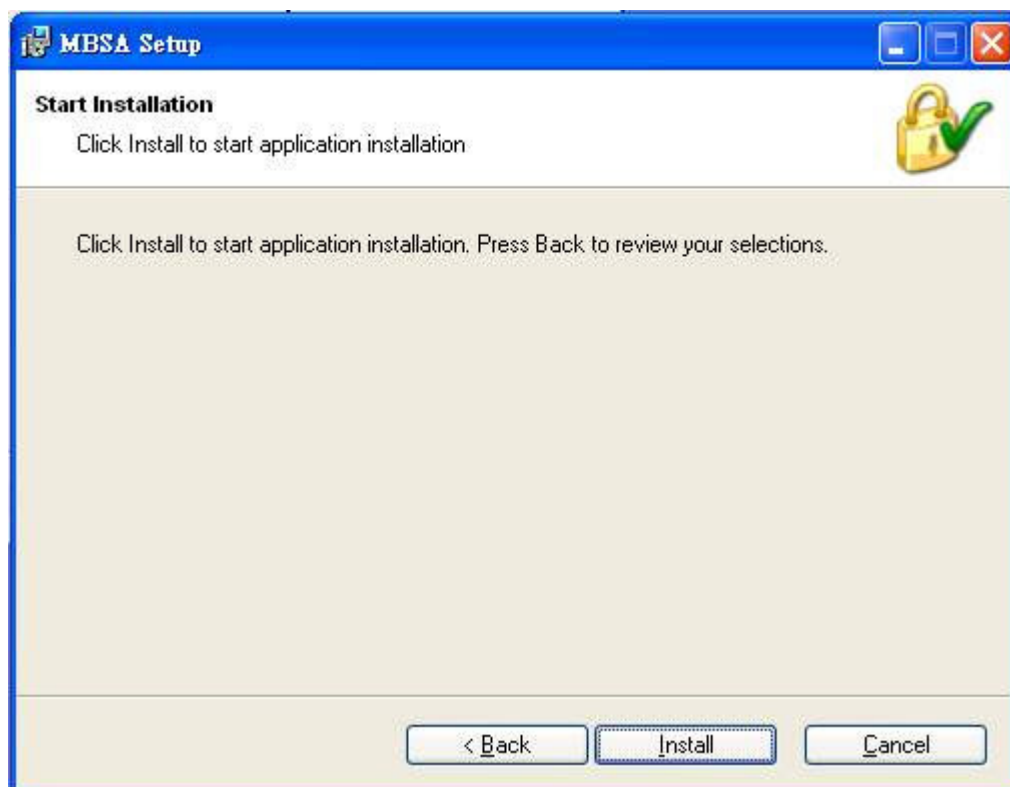
請按 [Next] 進行下一步安裝。



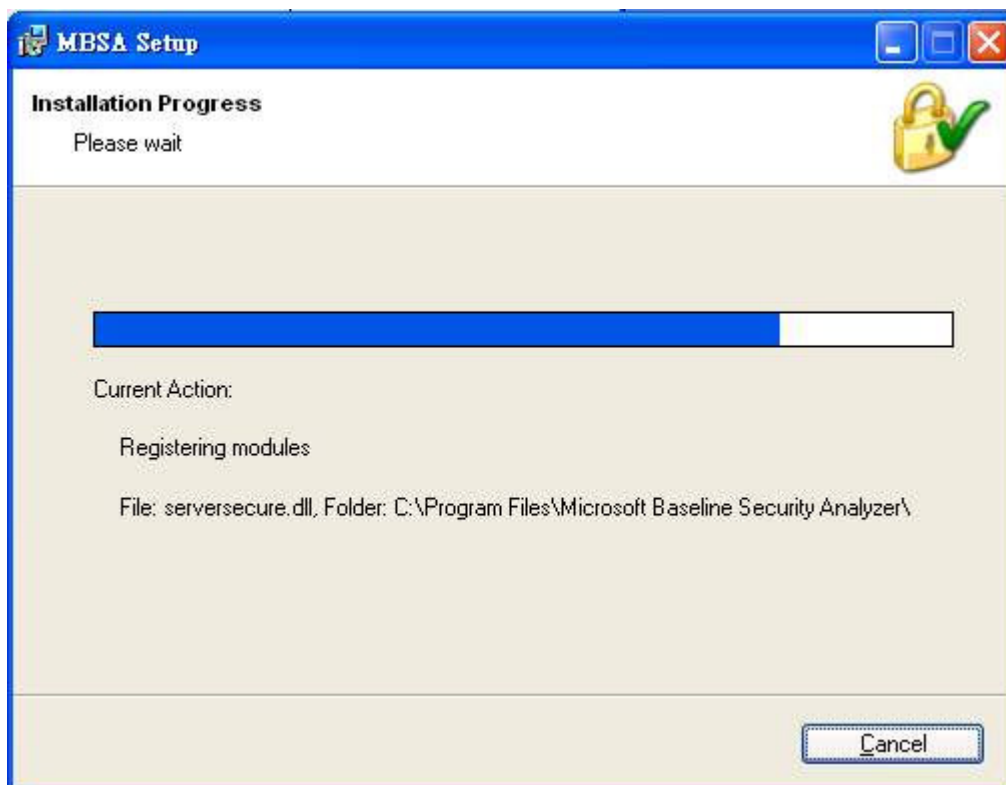
請點選[I accept the license agreement],然後點選[Next]。



預設安裝路徑為 C:\Program Files\Microsoft Baseline Security Analyzer ,請按[Next]繼續安裝。



請按[Install]開始安裝。



已經安裝完成的進度。



安裝完成,請按[OK]結束安裝程序。

五.MBSA 系統安全漏洞檢測:

Microsoft Baseline Security Analyzer

Microsoft
Baseline Security Analyzer

Microsoft Baseline Security Analyzer

- Welcome
- Pick a computer to scan
- Pick multiple computers to scan
- Pick a security report to view
- View a security report

See Also

- Microsoft Baseline Security Analyzer Help
- About Microsoft Baseline Security Analyzer
- Microsoft Security Web site

Welcome to the Microsoft Baseline Security Analyzer

The Microsoft Baseline Security Analyzer checks computers running Microsoft Windows® Server 2003, Windows XP, Windows 2000, or Windows NT® 4.0 for common security misconfigurations. You must have administrator privileges for each computer you want to scan.

Scans can be performed locally and remotely against computers running Windows Server 2003, Windows XP, Windows 2000, and Windows NT. Note that on computers running Windows XP and using simple file sharing, only local scans can be performed.

- Scan a computer
- Scan more than one computer
- View existing security reports

此畫面即為 MBSA 系統安全漏洞檢測畫面,請點選 [Scan a computer] 進行系統安全檢測程序。

Microsoft Baseline Security Analyzer

Microsoft
Baseline Security Analyzer

Microsoft Baseline Security Analyzer

- Welcome
- Pick a computer to scan
- Pick multiple computers to scan
- Pick a security report to view
- View a security report

See Also

- Microsoft Baseline Security Analyzer Help
- About Microsoft Baseline Security Analyzer
- Microsoft Security Web site

Pick a computer to scan

Specify the computer you want to scan. You can enter either the computer name or its IP address.

Computer name: WORKGROUP\DAK.XP (this computer)

IP address:

Security report name: %D% - %C% (%T%)

%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

Options:

- Check for Windows vulnerabilities
- Check for weak passwords
- Check for IIS vulnerabilities
- Check for SQL vulnerabilities
- Check for security updates
- Use SUS Server:

Learn more about Scanning Options

Start scan

勾選你要檢查的部分,然後按[Start scan]進行安全檢測程序。

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer

Scanning...

Currently scanning WORKGROUP\DARK\XP

Stop

Microsoft Baseline Security Analyzer

- Welcome
- Pick a computer to scan
- Pick multiple computers to scan
- Pick a security report to view
- View a security report

See Also

- Microsoft Baseline Security Analyzer Help
- About Microsoft Baseline Security Analyzer
- Microsoft Security Web site

開始進行系統漏洞檢測掃描程序。

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer

View security report

Sort Order: Score (worst first) ▼

Computer name: WORKGROUP\DARK\XP
 IP address: 192.168.1.101
 Security report name: WORKGROUP - DARK\XP (2004-12-10 下午 11:26)
 Scan date: 2004/12/10 下午 11:26
 Scanned with MBSA version: 1.2.4013.0
 Security update database version: 2004.12.01.0
 Office update database version: 11.0.0.7104
 Security assessment: Incomplete Scan (Could not complete one or more requested checks.)

Security Update Scan Results

Score	Issue	Result
✗	Windows Security Updates	2 critical security updates are missing. What was scanned Result details How to correct this
✗	Microsoft VM Security Updates	1 critical security updates are missing. What was scanned Result details How to correct this
✗	Office Updates	7 updates are missing. What was scanned Result details How to correct this
✓	Windows Media Player Security Updates	No critical security updates are missing. What was scanned
✓	MDAC Security Updates	No critical security updates are missing. What was scanned

Microsoft Baseline Security Analyzer

- Welcome
- Pick a computer to scan
- Pick multiple computers to scan
- Pick a security report to view
- View a security report

See Also

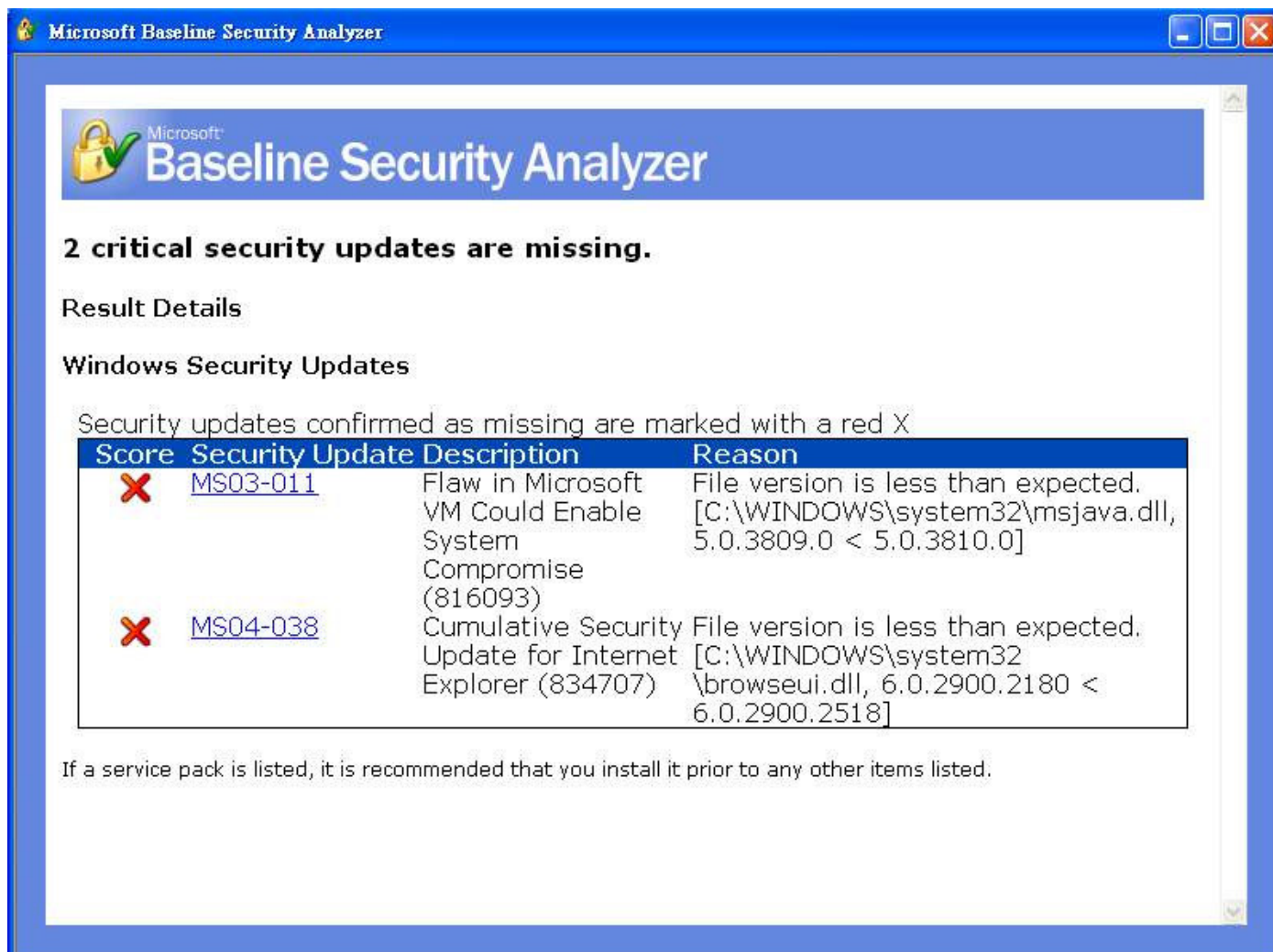
- Microsoft Baseline Security Analyzer Help
- About Microsoft Baseline Security Analyzer
- Microsoft Security Web site

Actions

Print

Copy

檢查完畢後,會出現如上畫面,打 X 部分是檢測出有安全性的漏洞需進行修補,打勾是表示通過檢查。



Microsoft Baseline Security Analyzer

Microsoft
Baseline Security Analyzer

2 critical security updates are missing.

Result Details

Windows Security Updates

Security updates confirmed as missing are marked with a red X

Score	Security Update	Description	Reason
X	MS03-011	Flaw in Microsoft VM Could Enable System Compromise (816093)	File version is less than expected. [C:\WINDOWS\system32\msjava.dll, 5.0.3809.0 < 5.0.3810.0]
X	MS04-038	Cumulative Security Update for Internet Explorer (834707)	File version is less than expected. [C:\WINDOWS\system32\browseui.dll, 6.0.2900.2180 < 6.0.2900.2518]

If a service pack is listed, it is recommended that you install it prior to any other items listed.

用滑鼠按下 "Result Details" 就會出現更詳細的安全性的漏洞說明。

Microsoft Baseline Security Analyzer - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 我的最愛

網址(D) C:\Program Files\Microsoft Baseline Security Analyzer\Help\check5311fix.html

Google 搜尋網頁 擷取彈出式視窗 選項

Microsoft Baseline Security Analyzer

Service Packs and Security Updates

Issue

To ensure that the most recent security updates are applied, you need to install all of the latest service packs and individual updates on your system.

Solution

The scan report identifies which service packs and security updates are missing on your computer. Users can click the link in the security report to view the Microsoft security bulletin or download page, which includes the install location for the security update. The [Windows Update](#) Web site also has the latest service pack and update releases available for you to download for the Microsoft® Windows® operating system and its components.

In order to obtain and install the latest updates and to effectively use the MBSA results, please observe the <http://www.microsoft.com/>

- Register with the [Microsoft Security Notification Service](#) to ensure you are notified when new security bulletins become available.
- When updating your computer, remember that changes in configuration may require additional use of Windows Update or MBSA to check the new configuration compliance. This is particularly true when installing applications, or adding new optional components such as Internet Information Services (IIS) which may include programs that have not been updated with the latest fixes.
- By clicking on **Result Details** in the report you will be able to identify the update as being under one of the following 3 headings:
 - Security updates confirmed as missing are marked with a red X**

These updates require immediate installation to ensure the strongest security of your computer.

若用滑鼠按下 "How to correct this" 請根據指示按"Windows Update"進行安全性的漏洞更新。

Microsoft Windows Update - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 我的最愛

網址(D) http://w5.windowsupdate.microsoft.com/v5consumer/default.aspx?ln=zh-tw

Google 搜尋網頁 擷取彈出式視窗 選項

台灣微軟網站 | 網站導覽

搜尋 Microsoft.com 網站的:

Windows Update

首頁 | Windows 系列 | Windows 類別目錄 | Office 系列

安裝更新

其他選項

- 檢視安裝記錄
- 設定
- 還原隱藏的更新
- 系統管理員選項
- 說明及支援
- 常見問題集

檢查最新版本 Windows Update 軟體...

視您的連線速度而定，此作業將花一些時間。在此期間，您可能收到一個或多個安全性警告。請詳加檢視每個安全性警告，確定該內容經數位簽章，然後按一下 [安裝] 或 [是] 開始安裝。

進行 Windows Update 安全性的漏洞更新檢查。

Microsoft Windows Update - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 · → 下一頁 · 搜尋 我的最愛

網址(D) http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx?ln=zh-tw

Google 搜尋網頁 擱載彈出式視窗 選項

台灣微軟網站 | 網站導覽

搜尋 Microsoft.com 網站的：

Windows Update

首頁 | Windows 系列 | Windows 類別目錄 | Office 系列

安裝更新 (2)

- 檢視高優先順序的更新 (2)
- 選取選用的軟體更新 (4)
- 選取選用的硬體更新 (1)

其他選項

- 檢視安裝記錄
- 設定
- 還原隱藏的更新
- 系統管理員選項
- 說明及支援
- 常見問題集

自訂安裝

檢視高優先順序的更新

高優先順序的更新是重大且與安全性相關的更新。

Microsoft 強烈建議您安裝下列高優先順序的更新，以便協助您的電腦保持在最新與安全的狀態。若要安裝這些更新，請按一下 [移至安裝更新]。

選取的更新總數：2 個項目, 8 MB, 5 分 移至安裝更新

高優先順序的更新

Microsoft Corporation - Windows XP family

- KB8834707 : Internet Explorer for Windows XP Service Pack 2 積存安全性更新
下載大小：2.9 MB, 2 分
現在已經證實有一個安全性問題，攻擊者可能利用此問題侵入執行 Internet Explorer 的電腦並取得該電腦的控制權。您可以從 Microsoft 此更新，協助保護您的電腦。安裝此項目後，您可能必須重新啟動電腦。 [詳細資料...](#)
 隱藏此更新
- 816093 : Microsoft Virtual Machine (Microsoft VM) 安全性修正檔

檢查完成後會列出可用的更新套件,請點選 [移至安裝更新] 以進行安裝。

Microsoft Windows Update - Microsoft Internet Explorer

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 我的最愛

網址(D) http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx?ln=zh-tw

Google 搜尋網頁 擱載彈出式視窗 選項

台灣微軟網站 | 網站導覽

Microsoft Windows

搜尋 Microsoft.com 網站的:

Windows Update

首頁 | Windows 系列 | Windows 類別目錄 | Office 系列

安裝更新 (2)

- 檢視高優先順序的更新 (2)
- 選取選用的軟體更新 (4)
- 選取選用的硬體更新 (1)

其他選項

- 檢視安裝記錄
- 設定
- 還原隱藏的更新
- 系統管理員選項
- 說明及支援
- 當目前題

安裝更新

此網頁提供已選取要安裝之更新的摘要資訊。

Microsoft 強烈建議您安裝下列高優先順序的更新，以便協助您的電腦保持在最新與安全的狀態。若要安裝這些更新，請按一下 [安裝]。

選取的更新總數：2 個項目, 8 MB, 5 分 安裝...

高優先順序的更新

Microsoft Corporation - Windows XP family

- KB834707: Internet Explorer for Windows XP Service Pack 2 積存安全性更新
 下載大小：2.9 MB, 2 分
 現在已經證實有一個安全性問題，攻擊者可能利用此問題侵入執行 Internet Explorer 的電腦並取得該電腦的控制權。您可以從 Microsoft 此更新，協助保護您的電腦。安裝此項目後，您可能必須重新啟動電腦。 [詳細資料...](#)
 隱藏此更新
- 816093: Microsoft Virtual Machine (Microsoft VM) 安全性修正檔

請點選 [安裝] 以進行安全性的漏洞更新,安裝完成後記得重新開機。

其它有打 X 部分請依序經由上述程序進行漏洞修補。

當所有的漏洞都已經修補完成後,最後再執行一次 **MBSA** 系統安全漏洞檢測程式確保所有的漏洞均以修補完畢。