**鼎新電腦 中介層漏洞修補工具說明**

1. **說明：**

|  |
| --- |
| * **修補工具包含下列檔案：請執行以下檔案**   **WebSecurityIssueFixer.exe** 執行檔  **為確保程式執行正常，請以系統管理員登入作業系統執行程式，及**以系統管理員身份執行程式。  以系統管理員   * **注意事項：**   此工具必須放置於欲修補系統其安裝路徑所在的磁碟中。  例：修補系統安裝於 D:\XXX\，則此工具就必須放置於 D: 磁碟中的某個路徑下。  執行時若出現，未安裝.NET Framework3.5的錯誤，請洽客服或產中協助。   * **指定修補的文件：**   此工具執行修補時，會將內嵌於 exe 中的 web.xml 更新至 JBoss 對應資料夾中，如果其內嵌的 web.xml 內容不正確，可以在 WebSecurityIssueFixer.exe 所在路徑下，建立一個子資料夾 "fixedData"，並且將正確的 web.xml 放置於其中，如此，工具修補時，就會使用此 web.xml 對 JBoss 進行更新。  **\*移除Jboss漏洞：**[JBOSS HOME]\...\...\...\jms\jbossmq-httpil.sar。  **\*移除異常程式：**檢查**[JBOSS HOME]/bin**，**C:\Users\Administrator\AppData\Local\Temp**，**C:\Windows\Temp**，及RAM中的相關執行緒，這些路徑下是否有異常程式(包含.vbs、.exe等)，目前較常發現的是：(3.exe、hu4.vbs、yam.exe、xmrig.exe、jaav.exe、ie.exe)等檔案。 |
|  |

1. **修補步驟：**

****

|  |
| --- |
| 1. **指定系統：**   選擇欲修補的系統，對於 WIP 和 eKB 而言，還可以勾選是否為進行測試區的修補動作。   1. **選擇安裝路徑：**   指定系統後，若修補工具無法獲取機碼取得安裝路徑，可手動點選資料夾瀏覽窗口自行選擇正確的安裝路徑。當 WIP 或是 eKB進行修補時，如果勾選了測試區，實際搜尋的路徑將會是 " [安裝路徑]\_TEST "。   1. **選擇JBoss Server 資料夾：**   下拉框中會顯示出安裝路徑下所有 JBoss開頭及各產品安裝的的資料夾名稱，請選取系統使用的JBoss資料夾。   1. **確認路徑後，請勾選確認路徑及資料夾正確** 2. **執行修補[點擊執行!]：**   修補完成後，可看見如下的對話框：  pic002.gif  在 log 中，可看見如下的信息：  QQ截圖20171206112325  當工具修補失敗時，你會看見如下的對話框：  pic004.gif  錯誤信息可能如下：  [錯誤1]：  pic005.gif  上述問題是因為安裝路徑下找不到 JBoss 的 web.xml 進行修補。  [錯誤2]：  pic006.gif  上述問題是因為工具放置於磁碟C，但是系統安裝路徑是在磁碟D中。   1. **驗證：針對目前修補的產品進行驗證**   [驗證!] 可以用來驗證目前的 Server 是否在下列 url 中存在安全性的漏洞：  http://127.0.0.1:999/invoker/JMXInvokerServlet  http://127.0.0.1:999/jmx-console  http://127.0.0.1:999/jmx-console/HtmlAdaptor  http://127.0.0.1:999/web-console  http://127.0.0.1:999/status?full=true  http://127.0.0.1:999//jbossmq-httpil/HTTPServerILServlet  上述 url中的 999 是在工具中的 port: 文字框中指定，執行驗證前，請先核對是否為 Server 所使用的 port，以免產生不正確的驗證結果。  操作：勾選**確認服務已經啟動**，點選**驗證**，當驗證成功後，可看見如下的對話框：若在此主機有安裝另一產品，可點選繼續修補下一個系統。  **QQ截圖20171206113644**  在 log 中，可看見如下的驗證成功訊息：  **QQ截圖20171206113655**  當驗證失敗時，你會看見如下的對話框：  pic010.gif  錯誤信息可能如下：  [錯誤1]：  pic011.gif  上述問題有可能是下列兩點原因所造成的：   1. port 號不正確：請檢查Server使用的port號，並且於工具中修正後，再重新點擊[驗證!]。 2. Server 還未開啟完成：請稍待片刻再重新點擊[驗證!]。   [錯誤2]：  上述的 url 其狀態顯示"開啟中"或是"狀態不明"，遇到此問題時，必須依照原標準程序手動處理，**若無法確定問題請反應給相關人員和客服或產中**。  QQ截圖20171206114034  或是  QQ截圖20171206140217   1. **備份路徑(此步驟可省略,不需檢查)：**   當修補完成後，工具所在路徑下會建立一個 rvytmp (意指Recovery Temp)資料夾，在此資料夾下，還會依據選擇的系統建立一個子資料夾，如下：  pic007.gif  資料夾中的 http-invoker.sar、jmx-console.war和 management 子資料夾都是原先在JBoss Server 中存在安全性漏洞的相關資源，而 .xml檔案則是修補前的 JBoss Server web.xml配置文件，工具將其名稱改為 web\_bk.xml。 |