在IIS 4.0和5.0的Microsoft Index Server ISAPI擴展中使用Cisco Secure IDS/NetRanger自定義字串匹配簽名來處理「紅色代碼」蠕蟲遠端緩衝區溢位

目錄

簡介

截至2003年7月底，Computer Economics（加利福尼亞州卡爾斯巴德的一個獨立研究機構）估計，「紅色代碼」蠕蟲已導致公司損失12億美元（美國）來恢復網路損壞和工作效率損失。隨著更強大的「紅色代碼II」蠕蟲的發佈，這一估計值大幅上升。作為Cisco SAFE藍圖的關鍵元件，思科安全入侵檢測系統(IDS)已證明其在檢測和降低網路安全風險（包括「紅色代碼」蠕蟲）方面的價值。

本文檔介紹用於檢測「紅色代碼」蠕蟲使用的攻擊方法的軟體更新(請參閱下面的簽名2)。

您可以建立如下所示的自定義字串匹配簽名，以捕獲運行Microsoft Windows NT和Internet Information Services(IIS)4.0或Windows 2000和IIS 5.0的Web伺服器利用緩衝區溢位漏洞的情況。另請注意，Windows XP beta中的索引服務也存在漏洞。描述此漏洞的安全建議位於 http://www.eeye.com/html/Research/Advisories/AD20010618.html 。Microsoft已發佈此漏洞的修補程式，可從http://www.microsoft.com/technet/security/bulletin/MS01-033.mspx 下載。

本文檔中討論的簽名在簽名更新版本S(5)中提供。 Cisco Systems建議在實施此特徵碼之前，將感測器升級到2.2.1.8或2.5(1)S3特徵碼更新。註冊使用者可從Cisco Secure Software Center下載這些特徵碼更新。所有使用者均可通過思科全球聯絡人通過電子郵件和電話聯絡思科技術支援。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據以下軟體版本：

- Microsoft Windows NT和IIS 4.0
- Microsoft Windows 2000和IIS 5.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

自定義字串匹配簽名

有兩個特定的自定義字串匹配簽名來解決此問題。下面將介紹每個簽名，並提供適用的產品設定。

簽名1 — 試圖利用漏洞訪問索引伺服器

此簽名在索引伺服器ISAPI擴展中嘗試緩衝區溢位時觸發，同時嘗試向伺服器傳遞shell代碼以獲得原始代碼形式的特權訪問。此簽名僅在嘗試向目標服務傳遞外殼代碼以嘗試獲得完整的系統級訪問許可權時觸發。一個可能的問題是，如果攻擊者沒有嘗試傳遞任何shell代碼，而是試圖使IIS崩潰並建立拒絕服務，則不會觸發此簽名。

字串

```
[Gg][Ee][Tt].*[.][Ii][Dd][Aa][\x00-\x7f]+[\x80-\xff]
```

產品設定

- 發生次數：1
- 連接埠:80

註：如果有在其他TCP埠（例如，8080）上偵聽的Web伺服器，則需要為每個埠號建立單獨的自定義字串匹配。

- 建議的警報嚴重性級別：高（思科安全策略管理器）5(Unix Director)
- Direction:到

簽名2 — Index Server訪問緩衝區溢位「紅色代碼」蠕蟲

第二個特徵碼在索引伺服器ISAPI擴展中嘗試緩衝區溢位時觸發，同時嘗試向伺服器傳遞shell代碼，以便以「紅色代碼」蠕蟲使用的模糊形式獲得特權訪問。此特徵碼僅在試圖向目標服務傳遞shell代碼以嘗試獲得完整的SYSTEM級別訪問許可權時觸發。一個可能的問題是，如果攻擊者沒有嘗試傳遞任何shell代碼，而是試圖使IIS崩潰並建立拒絕服務，則不會觸發此簽名。

字串

```
[/]default[.]ida[?][a-zA-Z0-9]+%u
```

注意：上述字串中沒有空格。

產品設定

- 發生次數：1
- 連接埠:80

註：如果有在其他TCP埠（例如，8080）上偵聽的Web伺服器，則需要為每個埠號建立單獨的自定義字串匹配。

- 建議的警報嚴重性級別：高（思科安全策略管理器）5(Unix Director)
- Direction:到

有關Cisco Secure IDS的詳細資訊，請參閱Cisco Secure Intrusion Detection。

相關資訊

- **技術支援 — 路由器**
- **思科資安諮詢**
- **思科安全入侵偵測支援頁面**
- **技術支援 - Cisco Systems**