|  |
| --- |
| **{{ project\_name1 }}**  **{{ project\_name2 }}**  **{{ project\_name3 }}** |

**文件編號: {{ file\_no }}**

**V1.0版**

**{{ date\_ch }}**

**安碁資訊股份有限公司**

**文件制／修訂記錄**

| **版號** | **日期** | **說明** | **作者** | **修訂中** | **定稿** |
| --- | --- | --- | --- | --- | --- |
| 1.0 | {{ date\_dot }} | Auto | ACSI |  | V |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**【目　　錄】**

[壹、 關於本報告 4](#_Toc190259726)

[一、 報告說明 4](#_Toc190259727)

[貳、 報告概述 5](#_Toc190259728)

[一、 目的 5](#_Toc190259729)

[二、 檢測範圍 5](#_Toc190259730)

[三、 弱點掃描方式 5](#_Toc190259731)

[四、 弱點掃描工具 5](#_Toc190259732)

[五、 弱點等級定義 6](#_Toc190259733)

[參、 檢測結果說明 7](#_Toc190259734)

[一、 分析摘要 7](#_Toc190259735)

[二、 弱點分佈分析 7](#_Toc190259736)

[三、 風險主機排行列表 8](#_Toc190259737)

[四、 風險弱點分類排行列表 9](#_Toc190259738)

[肆、 弱點修補建議 10](#_Toc190259739)

# 關於本報告

## 報告說明

本報告為安碁資訊股份有限公司依貴我雙方約定之作業範圍進行主機狀態軟體掃描檢測服務，謹就本次作業所見之項目進行說明陳述，並就相關可供優化、精進之資安防護機制提出建議，以供 貴公司做為後續防護規劃之依循參考。

* 1. 盡責聲明

本報告所使用之分析與檢測手法，為當前資訊安全產業所通用之技術與工具，所有方法與技術均有其極限，也將隨科技進步而更新，本公司謹盡合理可能之最大努力，就所見所聞如實提出本報告，容或有不足之處，仍請考量當前科技所能達成之極限，予以諒解。

# 報告概述

## 目的

本次「主機弱點掃描服務」，針對 貴單位現有伺服器主機之作業系統進行全面性的弱點掃描與檢測作業。主要目的為評估 貴單位現階段所面臨之資訊安全現況與風險指數，以作為未來 貴單位執行系統安全強化的作業基礎與修補參考。

## 檢測範圍

本中心於下表所列之時段派員於 貴單位執行本次弱點掃描作業，掃描網段及發現之主機數列於下表內。

1. 檢測範圍及時間

| **開始時間** | **結束時間** | **掃描範圍** | **主機數** |
| --- | --- | --- | --- |
| {%tr for row in table\_tar\_info %} |  |  |  |
| {{ row.start }} | {{ row.end }} | {{ row.target }} | {{ row.count }} |
| {%tr endfor %} |  |  |  |

## 弱點掃描方式

本次弱點掃描作業分為內外網，外網由本中心工程師透過作業IP遠端執行；內網則提供弱點掃描工具放置貴單位內部環境，針對貴單位指定範圍內所有IP網段進行作業系統全面性掃描與檢測。檢測項目以作業系統之一般及重大安全漏洞（弱點）為主，為避免影響受檢測系統之正常運作，檢測項目中將不包含「深度安全檢查及驗證」項目，如DoS類型的消耗資源及拒絕服務等攻擊測試。

## 弱點掃描工具

Nessus® 為業界部署最廣泛的漏洞與系統設定評估產品。Nessus 可以進行高速探索、系統設定稽核、資產剖析、敏感性資料探索、修補程式管理整合和漏洞分析。Tenable 的漏洞研究團隊準確的依據環境需求，提供不斷更新的資料庫 (plugins)，目前已支援超過 59,000 個漏洞和系統設定檢查。Nessus 能擴展並適用於最大型的企業環境，而且部署十分容易。

Nessus 至今已獲超過一千萬人下載，在資訊安全和法規遵循產品中，獲得眾多專業人士認可。目前所支援作業平台包括：

##### 網路裝置：Juniper、Cisco、Palo Alto Networks、防火牆、印表機等。

##### 虛擬主機：VMware ESX、ESXi、vSphere、vCenter。

##### 作業系統：Windows、Mac、Linux、Solaris、BSD、Cisco iOS、IBM iSeries。

##### 資料庫：Oracle、SQL Server、MySQL、DB2、Informix/DRDA、PostgreSQL。

##### Web 應用程式：Web 伺服器、網路服務、OWASP 漏洞。

##### 入侵偵測：病毒、惡意軟體、後門程式與受到殭屍網路感染之系統通訊的主機、連結至惡意內容的網路服務IPv4/IPv6 混合式網路等。

## 弱點等級定義

* 嚴重：屬重大漏洞的安全弱點，對系統有立即性威脅性。
* 高度：屬漏洞等級的安全弱點，對系統有高度威脅性。
* 中度：中度風險弱點，未提升至漏洞等級，觀察即可。
* 低度：低度風險弱點，威脅性甚低，可忽略。

# 檢測結果說明

## 分析摘要

本次掃描結果共有 {{ number\_total }} 個弱點總數，其中有 {{ number\_crit }} 個嚴重風險弱點，主要為 {{ va\_summary }}等弱點，建議儘速參考修補建議進行Patch更新作業，高度風險弱點請評估後進行修補。

## 弱點分佈分析

以下表列出本次掃描結果各風險等級弱點數目及總和。

1. 各等級風險弱點分佈

| **風險等級** | **嚴重** | **高** | **中** | **低** | **總計** |
| --- | --- | --- | --- | --- | --- |
| {%tr for row in table\_va\_summary %} |  |  |  |  |  |
| 弱點數 | {{ row.crit }} | {{ row.high }} | {{ row.med }} | {{ row.low }} | {{ row.total }} |
| {%tr endfor %} |  |  |  |  |  |

|  |
| --- |
| {{ summary\_image }}   1. 弱點等級分布柱狀圖 |

1. 各等級主機風險表

| **風險等級** | **嚴重** | **高** | **中** | **低** |
| --- | --- | --- | --- | --- |
| {%tr for row in table\_va\_summary\_host %} |  |  |  |  |
| 主機數 | {{ row.host\_crit }} | {{ row.host\_high }} | {{ row.host\_med }} | {{ row.host\_low }} |
| {%tr endfor %} |  |  |  |  |

|  |
| --- |
| {{ summary\_host\_va }}   1. 主機風險分布柱狀圖 |

## 風險主機排行列表

以下依IP Address排序，表列存在風險弱點等級之弱點數。

主機管理人員可參考第參章弱點修補建議，以IP Address為索引，找出該弱點對應之說明及修補建議等相關資訊，依建議進行主機弱點修補。

1. 各主機弱點數分佈

| **序號** | **IP Address** | **弱點分佈** | | | | **弱點總數** |
| --- | --- | --- | --- | --- | --- | --- |
| **嚴重** | **高** | **中** | **低** |
| {%tr for row in table\_va\_count %} |  |  |  |  |  |  |
| {{ row.no }} | {{ row.ip }} | {{ row.crit }} | {{ row.high }} | {{ row.med }} | {{ row.low }} | {{ row.total }} |
| {%tr endfor %} |  |  |  |  |  |  |

## 風險弱點分類排行列表

以下依弱點等級排序，表列本次檢測發現之風險弱點。可依據該弱點對應編號，參考第參章弱點修補建議，查詢該弱點對應之說明及修補建議等相關資訊。

1. 各等級風險弱點數分佈

| **序號** | **弱點 等級** | **弱點編號** | **弱點名稱** | **出現**  **數目** |
| --- | --- | --- | --- | --- |
| **{%tr for row in table\_va\_sum %}** |  |  |  |  |
| {{ row.no }} | {{ row.risk }} | {{ row.pluginnum }} | {{ row.pluginname }} | {{ row.count }} |
| {%tr endfor %} |  |  |  |  |

# 弱點修補建議

本章提供本次掃描所發現之風險弱點，其風險原因及建議修補方式，另外提供附件予主機或系統管理單位可依據所提供之資訊，進行有效之弱點修補作業。