

DNS Security in Taiwan

台灣網路資訊中心(TWNIC) 楊禎葆、台灣電腦網路危機處理中心(TWCERT) 賴冠州

摘要

本計畫案由台灣網路資訊中心(TWNIC)委託台灣電腦網路危機處理中心(TWCERT)，進行台灣地區網域名稱伺服器安全性的調查，檢測 ISC BIND 的版本分佈情形，並針對相關版本做弱點資訊的分析與統計，而後提出安全建議與改進方案。調查結果將作為提升台灣地區網域名稱伺服器安全性的參考。

關鍵字：

網域名稱伺服器、弱點掃描、網路安全、BIND、DNS、ISC

1. 前言

於 2001 年 5 月 12 日檢測台灣地區 ISC BIND 的版本分佈情形，並針對相關版本做弱點資訊的分析與統計，提出改進方案。在第二章我們會針對檢測方法做一個說明；第三章將詳細分析台灣地區的 ISC BIND 的版本分佈情形；第四章則是探討 ISC BIND 弱點的相關資訊和分佈狀況；第五章會提出詳細的檢測結果分析；在最後一章我們將歸納成幾個部分，提出詳細的改進方案與安全建議。

2. 安全檢測方法

針對 TWNIC 的 ROOT DNS 的 NS 記錄，使用 dig 指令查詢 version 資訊，共檢測出 16,510 部 DNS 伺服器。並針對相關的版本做弱點資訊的整理、統計與分析。

3. DNS 版本分佈情形

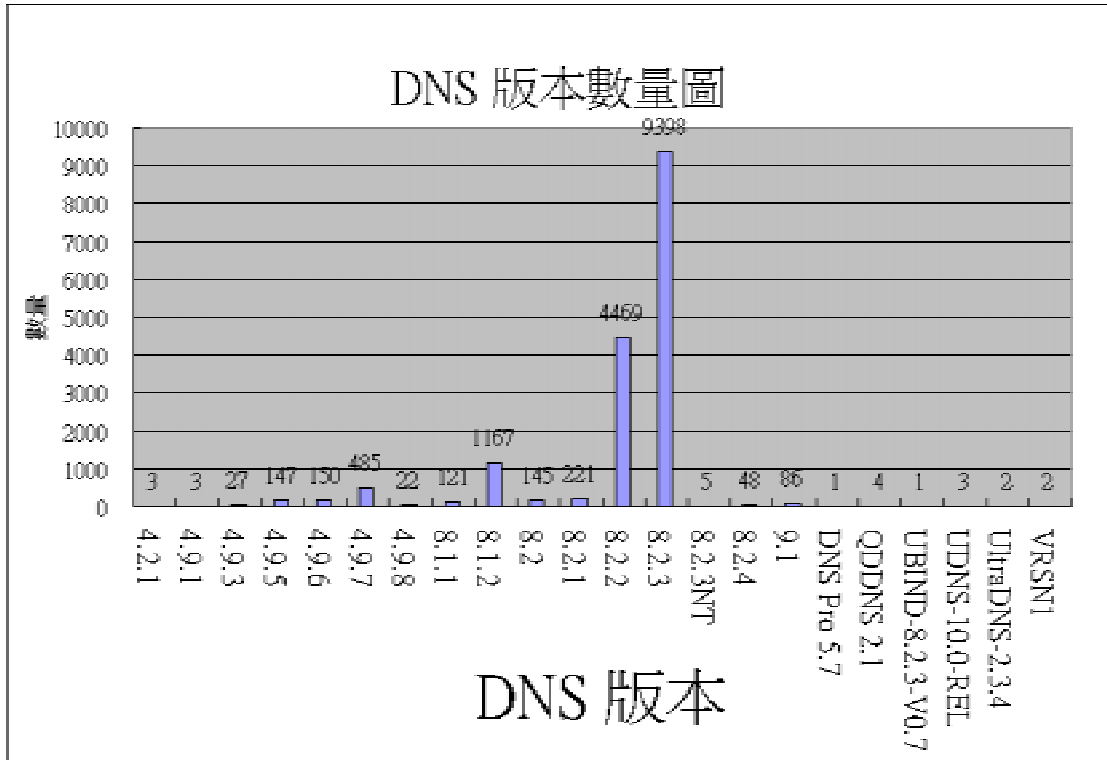
3.1 BIND 的歷史

根據 ISC 的統計資料指出，目前 ISC BIND 是全世界使用最多的 DNS 伺服器軟體。從最早期的 v4 版本開始，目前只剩 OpenBSD 繼續使用 v4，所以有很多新的功能在 v4 裡面並沒有出現，當然這也是 OpenBSD 支持者繼續採用 v4 的原因。除此之外，最常用的版本就是 v8 了，BIND 8 目前穩定的版本是 8.2.4。之後，就是全新改寫的版本 v9。BIND 9 在 2000 年 10 月推出，也是完全免費，但受到商業公司的贊助，目前穩定的版本是 9.1.3，修正了 9.1.2 部分的 bugs，但未添加新的功能。而 9.2.0rc1 則是 9.2.0 最新的候補版本。

3.2 台灣地區分佈情形

以 ISC BIND 為 DNS 版本列表，主要為適用於 UNIX-base 之平台，亦有少數的 WINDOWS 版。所查詢之結果 .tw 為 ROOT DNS 之所有 NS 記錄，餘則以各別之第二層為主(含.net)，故有差額。

.gov.tw	.com.tw	.edu.tw	.net.tw	.org.tw	.idv.tw	.net	總數
206	11,845	412	434	488	1,064	538	14987

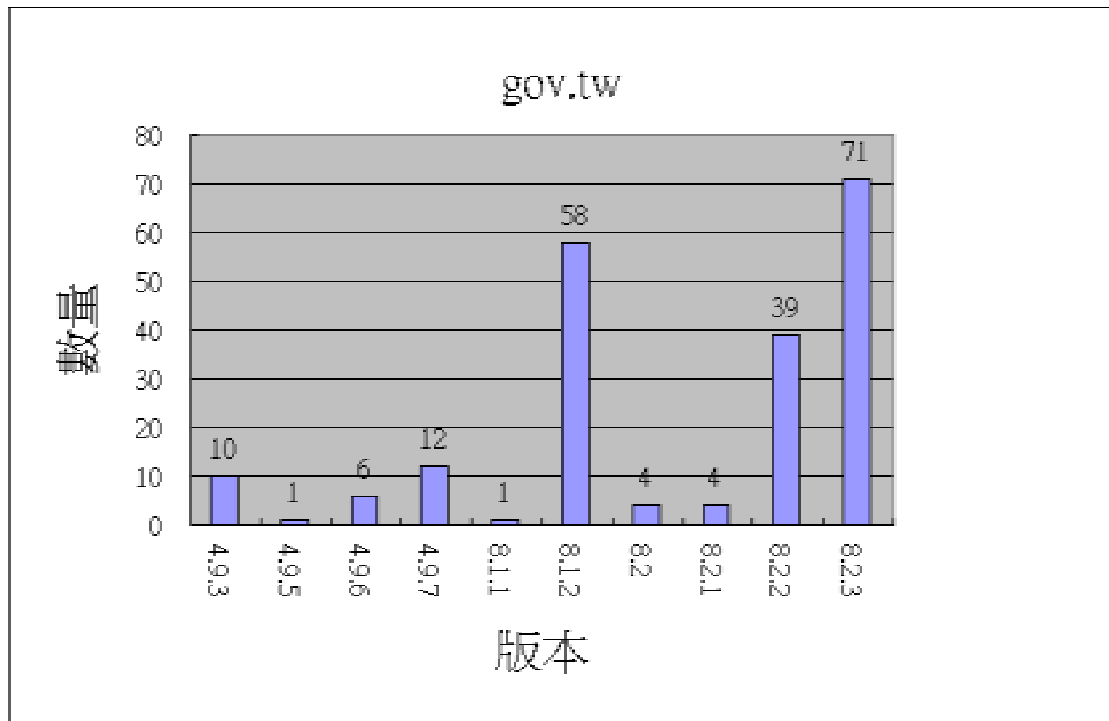


圖(一) 台灣地區的 DNS 版本分佈圖 (TWNIC 提供)

DNS 版本	數量	比例(%)
4.2.1	3	0.02
4.9.1	3	0.02
4.9.3	27	0.16
4.9.5	147	0.89
4.9.6	150	0.90
4.9.7	485	2.94
4.9.8	22	0.13
8.1.1	121	0.73
8.1.2	1167	7.06
8.2	145	0.88
8.2.1	221	1.34
8.2.2	4469	27.07
8.2.3	9398	56.92
8.2.3NT	5	0.03

8.2.4	48	0.29
9.1	86	0.52
DNS Pro 5.7	1	0.01
QDDNS 2.1	4	0.02
UBIND-8.2.3-V0.7	1	0.01
UDNS-10.0-REL	3	0.02
UltraDNS-2.3.4	2	0.01
VRSN1	2	0.01
共 22 種版本 (已去除重複部分)	16510	100%

表(一) 台灣地區的 DNS 版本統計圖表

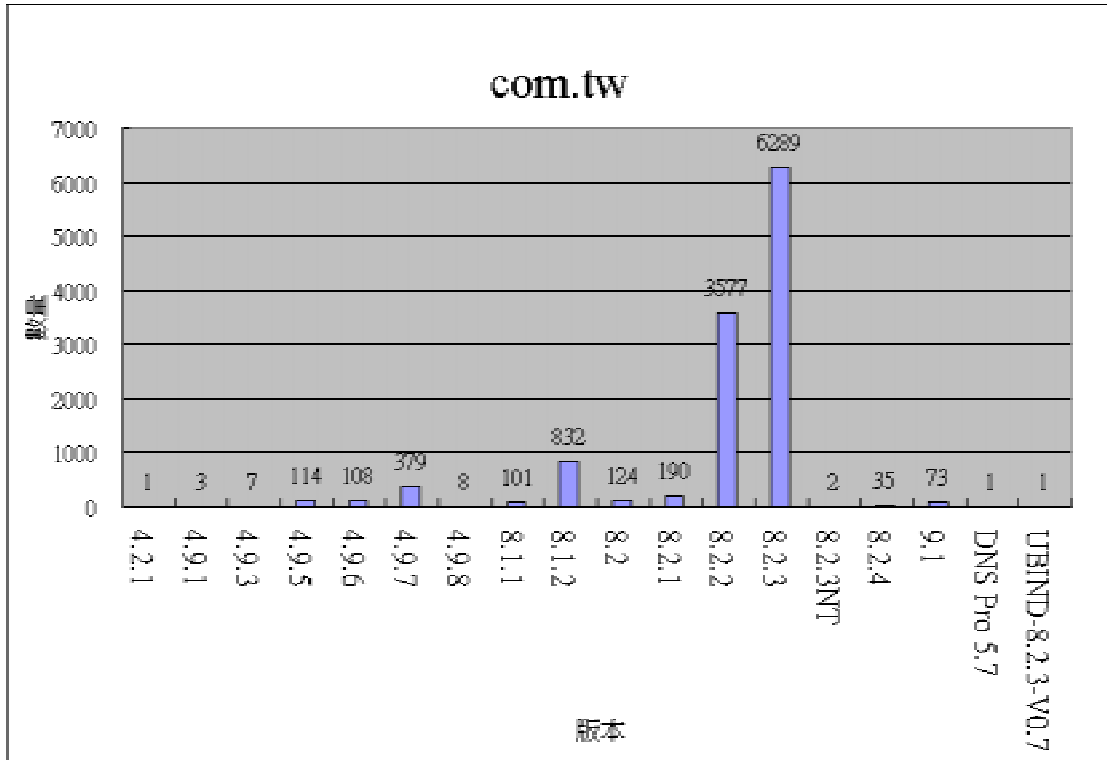


圖(二) 台灣地區政府單位(.gov.tw)的 DNS 版本分佈圖 (TWNIC 提供)

DNS 版本	數量	比例(%)
4.9.3	10	4.85
4.9.5	1	0.49
4.9.6	6	2.91
4.9.7	12	5.83
8.1.1	1	0.49
8.1.2	58	28.16
8.2	4	1.94
8.2.1	4	1.94

8.2.2	39	18.93
8.2.3	71	34.47
共 10 種版本	206	100%

表(二) 台灣地區政府單位(.gov.tw)的 DNS 版本統計圖表

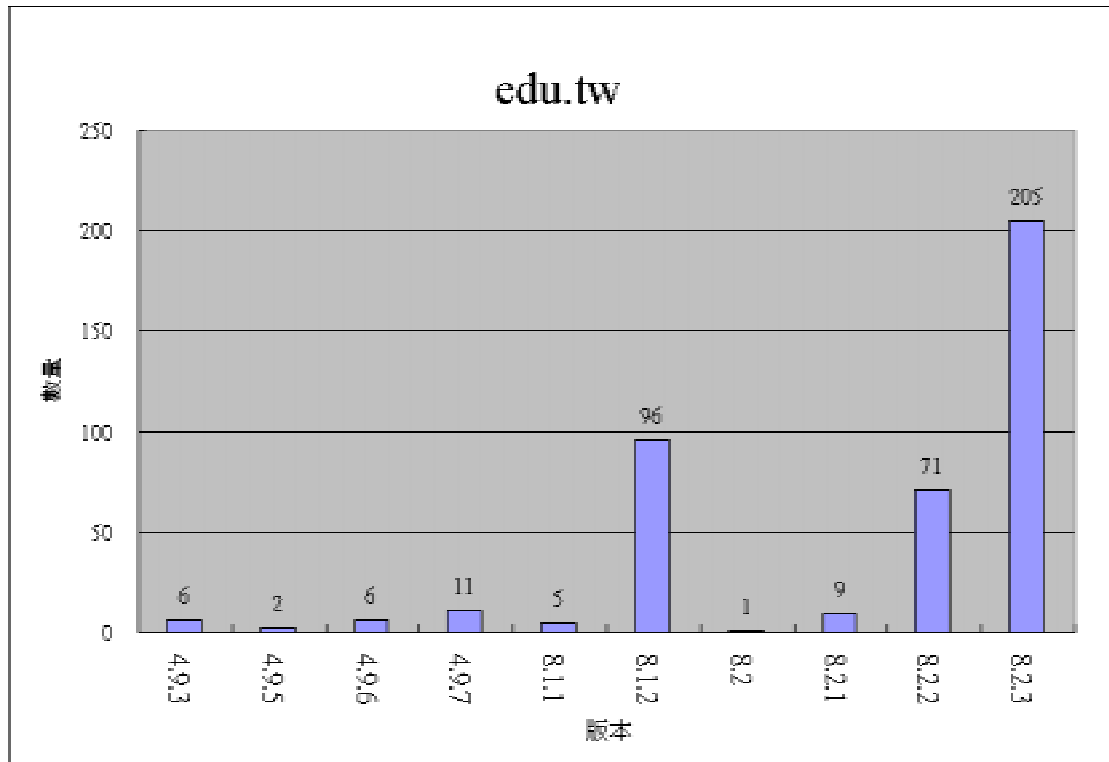


圖(三) 台灣地區商業機構(.com.tw)的 DNS 版本分佈圖 (TWNIC 提供)

DNS 版本	數量	比例(%)
4.2.1	1	0.01
4.9.1	3	0.03
4.9.3	7	0.06
4.9.5	114	0.96
4.9.6	108	0.91
4.9.7	379	3.20
4.9.8	8	0.07
8.1.1	101	0.85
8.1.2	832	7.02
8.2	124	1.05
8.2.1	190	1.60
8.2.2	3577	30.20
8.2.3	6289	53.09

8.2.3NT	2	0.02
8.2.4	35	0.30
9.1	73	0.62
DNS Pro 5.7	1	0.01
UBIND-8.2.3-V0.7	1	0.01
共 18 種版本	11845	100%

表(三) 台灣地區商業機構(.com.tw)的 DNS 版本統計圖表

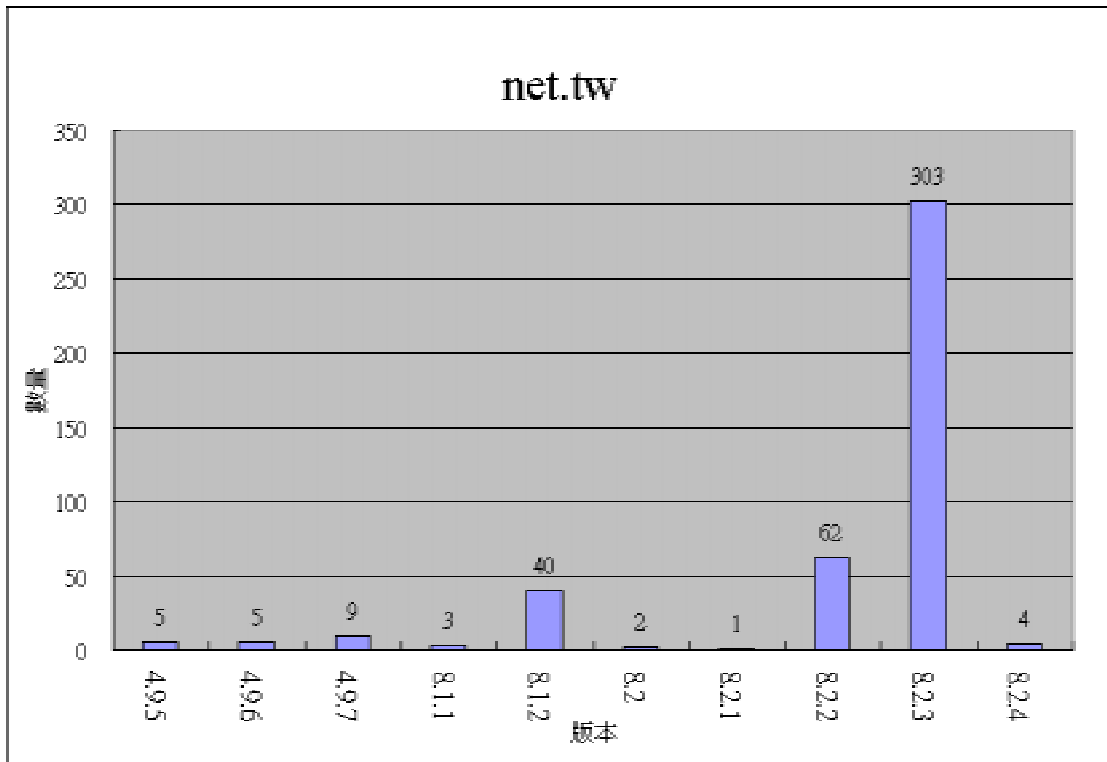


圖(四) 台灣地區教育單位(.edu.tw)的 DNS 版本分佈圖 (TWNIC 提供)

DNS 版本	數量	比例(%)
4.9.3	6	1.46
4.9.5	2	0.49
4.9.6	6	1.46
4.9.7	11	2.67
8.1.1	5	1.21
8.1.2	96	23.30
8.2	1	0.24
8.2.1	9	2.18
8.2.2	71	17.23
8.2.3	205	49.76

共 10 種版本	412	100%
----------	-----	------

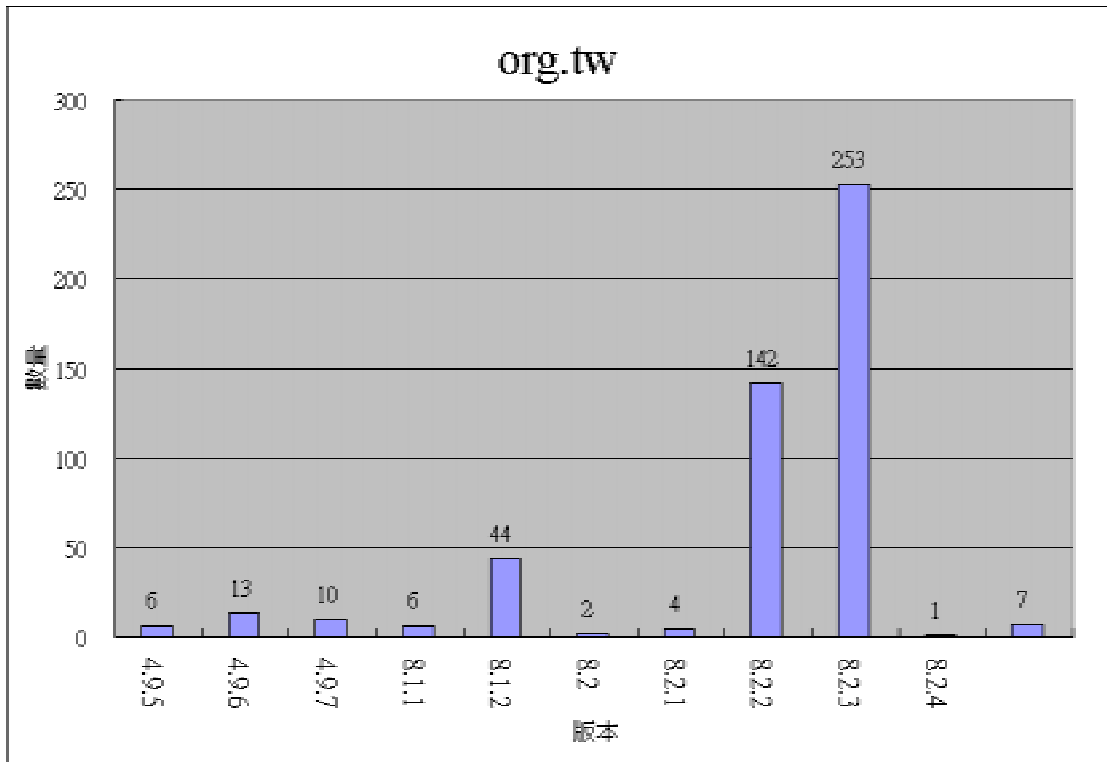
表(四) 台灣地區教育單位(.edu.tw)的 DNS 版本統計圖表



圖(五) 台灣地區網路服務單位(.net.tw)的 DNS 版本分佈圖 (TWNIC 提供)

DNS 版本	數量	比例(%)
4.9.5	5	1.15
4.9.6	5	1.15
4.9.7	9	2.07
8.1.1	3	0.69
8.1.2	40	9.22
8.2	2	0.46
8.2.1	1	0.23
8.2.2	62	14.29
8.2.3	303	69.82
8.2.4	4	0.92
共 10 種版本	434	100%

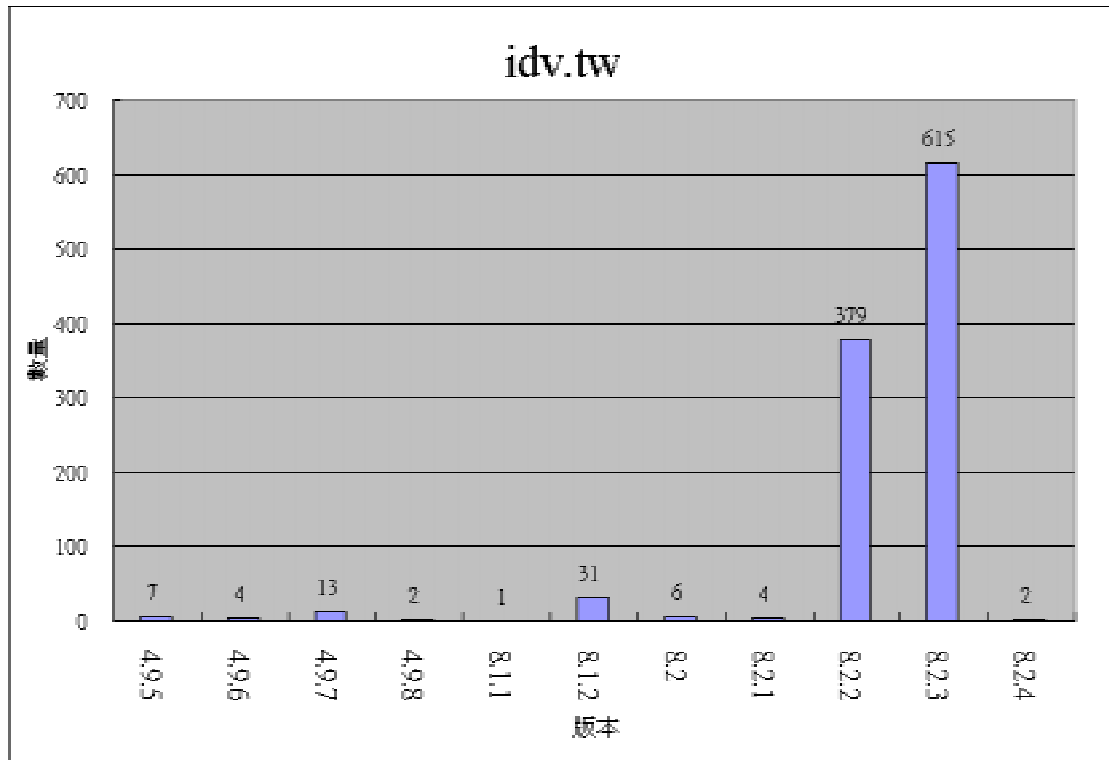
表(五) 台灣地區網路服務單位(.net.tw)的 DNS 版本統計圖表



圖(六) 台灣地區非營利組織(.org.tw)的 DNS 版本分佈圖 (TWNIC 提供)

DNS 版本	數量	比例(%)
4.9.5	6	1.23
4.9.6	13	2.66
4.9.7	10	2.05
8.1.1	6	1.23
8.1.2	44	9.02
8.2	2	0.41
8.2.1	4	0.82
8.2.2	142	29.10
8.2.3	253	51.84
8.2.4	1	0.20
9.1	7	1.43
共 11 種版本	488	100%

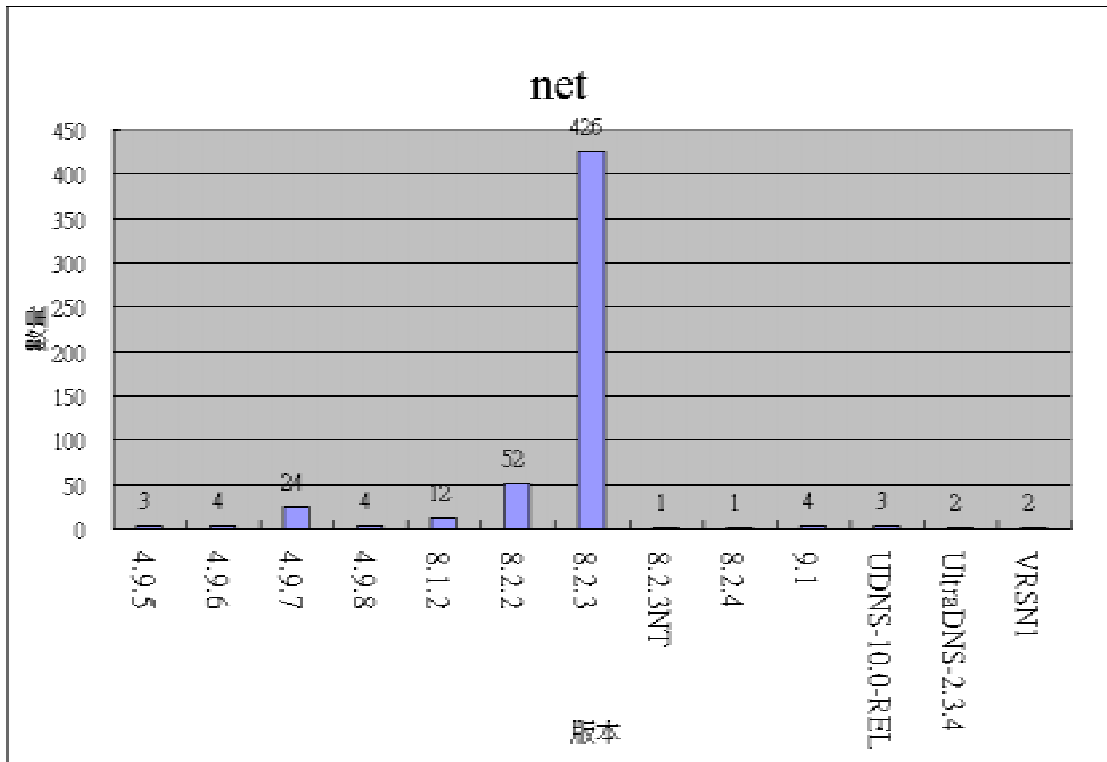
表(六) 台灣地區非營利組織(.org.tw)的 DNS 版本統計圖表



圖(七) 台灣地區個人申請(.idv.tw)的 DNS 版本分佈圖 (TWNIC 提供)

DNS 版本	數量	比例(%)
4.9.5	7	0.66
4.9.6	4	0.38
4.9.7	13	1.22
4.9.8	2	0.19
8.1.1	1	0.09
8.1.2	31	2.91
8.2	6	0.56
8.2.1	4	0.38
8.2.2	379	35.62
8.2.3	615	57.80
8.2.4	2	0.19
共 11 種版本	1064	100%

表(七) 台灣地區個人申請(.idv.tw)的 DNS 版本統計圖表



圖(八) TLD 屬於台灣地區網路服務單位(.net)的 DNS 版本分佈圖 (TWNIC 提供)

DNS 版本	數量	比例(%)
4.9.5	3	0.56
4.9.6	4	0.74
4.9.7	24	4.46
4.9.8	4	0.74
8.1.2	12	2.23
8.2.2	52	9.67
8.2.3	426	79.18
8.2.4	1	0.19
9.1	4	0.74
UDNS-10.0-REL	3	0.56
UltraDNS-2.3.4	2	0.37
VRSN1	2	0.37
共 13 種版本	538	100%

表(八) TLD 屬於台灣地區網路服務單位(.net)的 DNS 版本統計圖表

4. DNS 弱點分佈情形

版本	zxfr	sigdiv0	srv	nxt	sig	naptr	maxdname	solinger	fdmax	complain	inforeak	tsig
4.8	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	+	n/a
4.8.1, 4.8.2.1, 4.8.3	n/a	n/a	n/a	n/a	n/a	n/a	-	n/a	n/a	n/a	+	n/a
4.9.1	n/a	n/a	n/a	n/a	n/a	n/a	-	n/a	n/a	+	+	n/a
4.9.3	n/a	n/a	n/a	n/a	n/a	n/a	-	n/a	n/a	+	+	n/a
4.9.4 – 4.9.4p1	n/a	n/a	n/a	n/a	n/a	n/a	-	n/a	n/a	+	+	n/a
4.9.5	n/a	n/a	-	n/a	+	+	+	n/a	n/a	+	+	n/a
4.9.5 p1	n/a	n/a	-	n/a	+	+	+	n/a	n/a	+	+	n/a
4.9.6	n/a	n/a	-	n/a	+	+	+	n/a	n/a	+	+	n/a
4.9.7	n/a	n/a	-	n/a	-	+	+	n/a	n/a	+	+	n/a
4.9.8	n/a	n/a	-	n/a	-	+	+	n/a	n/a	-	-	n/a
8.1	n/a	n/a	-	n/a	+	+	+	+	+	-	+	n/a
8.1.1	n/a	n/a	-	n/a	+	+	+	+	+	-	+	n/a
8.1.2	n/a	n/a	-	n/a	-	+	+	+	+	-	+	n/a
8.2	-	+	+	+	+	+	+	+	+	-	+	+
8.2 p1	-	+	+	+	+	+	+	+	+	-	+	+
8.2.1	-	+	+	+	+	+	+	+	+	-	+	+
8.2.2	+	+	+	-	-	+	+	-	-	-	+	+
8.2.2 p1	+	+	+	-	-	+	+	-	-	-	+	+
8.2.2 p2 – p5	+	+	+	-	-	-	-	-	-	-	+	+
8.2.2 p6	+	-	+	-	-	-	-	-	-	-	+	+
8.2.2 p7	-	-	-	-	-	-	-	-	-	-	+	+
8.2.3	-	-	-	-	-	-	-	-	-	-	-	-
8.2.3NT	-	-	-	-	-	-	-	-	-	-	-	-
8.2.4	-	-	-	-	-	-	-	-	-	-	-	-
9.0.0	n/a	-	-	-	-	-	-	-	-	-	-	-
9.1.0	n/a	-	-	-	-	-	-	-	-	-	-	-

表(九) ISC BIND 各版本的弱點整理圖表 (反白區域表台灣地區所有的 DNS 版本；其中 '+' 表有弱點； '-' 表沒有弱點； 'n/a' 表無此項功能)

弱點資訊	Zxfr	sigdiv0	srv	Nxt	sig	naptr	Max dname	solinger	fdmax	complain	inforeak	tsig
數量	4,469	4,835	4,835	366	784	6,927	6,927	1,654	1,654	812	6,935	4,835

比例 (%)	27.06	29.29	29.29	2.22	4.75	41.96	41.96	10.02	10.02	4.92	42.00	29.29
--------	-------	-------	-------	------	------	-------	-------	-------	-------	------	-------	-------

表(十) 台灣地區 ISC BIND 各版本的弱點統計圖表

弱點名稱	弱點描述	解決方法
Buffer overflow in Transaction Signatures(TSIG)	BIND 8 在檢查 TSIG 時沒有處理好，回應錯誤訊息時導致緩衝區溢位的問題發生，可能會讓攻擊者取得超權限的授權，並執行任意的程式碼。	1. 將 BIND 升級到最新穩定的版本。(8.2.4 or 9.1.3) 2. 採用嚴格的加密法來做服務上的認證。
buffer overflow in nslookupComplain()	有弱點的 buffer 主要是用來暫存給 syslog 的錯誤訊息。攻擊者藉由傳送格式化的查詢字串，導致 BIND 4 緩衝區溢位的發生，並讓伺服器造成癱瘓或是取得超權限授權，而能執行任意的程式碼。	3. 水平切割 DNS zone，來降低衝擊。
Input validation error in nslookupComplain()	有弱點的 buffer 主要是用來暫存給 syslog 的錯誤訊息。攻擊者藉由傳送格式化的查詢字串，導致 BIND 4 緩衝區溢位的發生，並讓伺服器造成癱瘓或是取得超權限授權，而能執行任意的程式碼。	
Disclose environment variables	藉由送出格式化的查詢字串，導致 BIND 4 和 BIND 8 伺服器處理不當，洩漏了伺服器的相關資訊或是環境變數。	
Nxt bug	某些版本的 BIND 在驗證 NXT 記錄時失敗，入侵者可取得超權限授權，並執行任意的程式碼。	1. 將 BIND 升級到最新穩定的版本。 2. BIND 8.2.4
Sig bug	在驗證 SIG 記錄時失敗，導致 named 當掉。	3. BIND 9.1.3
So_linger bug	在結束 TCP session 時，入侵者藉由蓄意的違反通訊協定的規定，導致 named 暫停服務達 120 秒。	
Fdmax bug	藉由消耗大量的 file descriptors，可導致 named 當掉。	
Maxdname bug	不正常的處理從網路拷貝來的資料，可導致伺服器當掉。	

Naptr bug	某些版本的 BIND 在處理由磁碟載入的 zone information 時驗證失敗，可能導致 named 當掉。	
Inverse query buffer overflow	named 在做反查時沒有做緩衝區大小的檢查，可能使得拷貝資料時發生緩衝區溢位的問題。入侵者可藉由 TCP 協定送出查詢字串導致 named 當掉，甚至取得 root 權限。	<ol style="list-style-type: none"> 1. BIND 8：將設定檔 named.conf 裡面的 "fake-iquery" 完全移除。不需要設定 yes or no。 2. BIND 4.9：同 BIND 8 將該行設定移除，之後緊接著看原始碼裡的 conf/options.h，假如 INVQ 有被定義的話，請將它 comment 起來，並重新編譯和重新安裝 named 即可。
DoS vulnerability in BIND 4.9 and 8 release	藉由送出不正常或是惡意的格式化的 DNS 訊息，可能導致伺服器讀取到無效的記憶體位址，產生一些不正確的記錄，甚至導致伺服器當掉。很多的 DNS 工具程式(e.g. dig, nslookup)在處理 DNS 訊息時也沒有做記憶體範圍的檢查。	<ol style="list-style-type: none"> 1. 將 BIND 升級到最新穩定的版本。
DoS vulnerability in BIND 8 release	<pre>Foo.example IN A CNAME foo.example</pre> <p>以上例子可能會發生遞迴查詢的情形。一旦這個記錄存在 cache 中，當使用該領域名稱發出 zone transfer 要求時，可能會導致伺服器終止(abort)執行。雖然大部分的伺服器不太可能存在這樣的設定，但是攻擊者還是可以利用一些方法把這樣的紀錄放到 cache 裡，導致 DoS 狀況的發生。</p>	<ol style="list-style-type: none"> 1. 將 BIND 升級到最新穩定的版本。

表(十) DNS 安全性漏洞分析

5. 檢測結果分析

從第四章的弱點列表中我們可以歸納出幾種攻擊的模式：

1. Buffer overflow：即緩衝區溢位的攻擊，藉由傳送特定的 shell codes，可能會讓

攻擊者取得 named 執行時的權限或是 root 權限，執行惡意的指令。甚至在被入侵的主機開啟一個 remote login shell，即所謂的後門，以方便下次的入侵。例如在 2000 年 4 月間流傳的 lion worm(獅子網蟲)[9]即是。

2. Crash server：藉由傳送不正常的訊息，導致 named 處理時產生錯誤 crash 掉。
3. Denial of Service：藉由傳送不正常的封包或是因為系統管理者錯誤的設定，導致伺服器無法提供正常的服務，即阻斷服務攻擊(DoS attack)的發生。和 crash server 不同的是，這種攻擊模式並未造成伺服器當機，只是忙於處理『不正常的』requests。
4. Information leak：即洩漏伺服器資訊的攻擊方式。有心人士可以得知系統相關資訊，並擬定下一波的攻擊行動。

從上面的攻擊方式中，以 buffer overflow 的攻擊方式影響最為嚴重，其次是造成伺服器當機和 DoS 的攻擊，最後則為伺服器資訊的洩漏。而台灣地區最常使用的 DNS 版本前三名依次為 8.2.3 佔 56.92%、8.2.2 佔 27.07%和 8.1.2 佔 7.06%，整體比例已經超過了九成，其中是 8.2.3 就佔了一半以上。

從以上的版本統計資料再去對照相關版本的弱點資訊，並把其它尚未發現弱點的版本列入統計，我們可以得到一個明確的資訊，就是約有 42%的 DNS 伺服器是有弱點存在的，其中嚴重的弱點就佔了 30%，剩下的 12%則是屬於中低程度的危險，而所謂『安全的』伺服器則佔了 58%（目前尚未發現有弱點，並不代表以後不會有弱點）。

6. 安全建議與改進方案

對於 DNS 的威脅是很多面的，而根據 DeMorgan 在[7]的描述中主要可以分成以下三個重點來探討：機密性(confidentiality)、可利用性(availability)和整合性(integrity)。

所謂『機密性』就是經由 DNS 的封包是否會被竊聽？E-Mail 是否會被攔截？一旦有心人士入侵了該 DNS 伺服器，那麼所有的資料幾乎就保了，甚至連商業交易都可能被攔截、竄改。更進一步來說，該 DNS 伺服器可能被當成跳板，利用網域內的信任關係，去入侵其它的機器。

而『整合性』就是，入侵者可藉由竄改主要的 mail exchanger(MX)記錄，導致郵件路徑轉向入侵者設置的主機，而真正的郵件主機無法收到信件，藉此入侵者可以偽裝成你的身份，任意發佈信件、訊息，導致你的聲譽受損。另外也可以竄改 Web 伺服器的路徑，轉向入侵者設置的主機，藉此欺騙使用者以為是真正的主機，如此便可以竊取商業機密，例如信用卡資料、網路銀行帳號/密碼資料等等。最後一點就是『偽裝』(masquerading)，即入侵者不修改既有的 DNS 記錄，而加上一筆新的紀錄，這樣系統管理者很難發覺，但是入侵者卻可以利用該筆記錄的主機，偽裝成你其中的一部機器，去攻擊其它的電腦，事後追查起來時，可能會讓你背黑鍋。

『可利用性』即是，DNS 伺服器是非常重要的，任何時刻都應該維持正常的運作，一旦當機或是發生問題，不但 e-mail 無法正確寄達，連外面都無法連上你提供的服務。所以系統管理者應該時時刻刻注意主機是否遭人入侵？記錄是否遭到竊改，甚至刪除？以確保系統正常的運作。

總歸來說 DNS 的問題不外乎軟體的問題和人員的問題，就是採用了有弱點的軟體或是採用了技術不好的人員，導致系統設定發生問題。而為了解決以上所提出來的問題，根據[1][2]所提出來的改進方案，我們可以歸納整理成以下幾部分供各位參考。

6.1 一般性的建議

以下幾點供各位參考：

- 盡量採用最新版本的 BIND，並定時注意任何相關的安全通報，採用適當的 patch。目前穩定的版本是 8.2.3 和 9.1.2。
- 不要在 DNS 伺服器上提供其它的服務，此舉可降低其它服務可能造成的風險。
- 採用雙 DNS 系統，第二個當 secondary，避免主要伺服器失效時，還有備援伺服器可用，服務不中斷。
- 注意 access control，限制 zone transfer 的範圍，並盡可能採用 tsig(transaction signature)。
- 採用 chroot 的方式以最低權限啟動 named，不要用系統既有的帳號身份(例如 nobody 等)，以降低入侵成功時的風險，減少損失。並在啟動 named 時，
 1. 指定 `-r` 參數：關閉遞迴查詢的功能；
 2. 指定 `-u -g` 參數：設定程序執行時有效的使用者和群組，避免以 root 方式執行，降低被入侵成功時(例如 buffer overflow 的攻擊)造成的損害；
 3. 指定 `-t` 參數：指定 chroot()的目錄。
- 隱藏版本資訊。可欺騙一般的速成駭客(script kiddie)，避免他們直接拿網路上輕易取得的 exploits 程式隨意的攻擊他人。
- 隨時察看日誌檔(log)，檢查有無異狀。所謂早期發現早期治療，某些 buffer overflow 的攻擊，可能會讓系統造成 core dump，從系統日誌中可以得到些許蛛絲馬跡。

6.2 設定檔的修改

在 BIND 8 中有下列幾種方法可以增加安全性[1]：

- 在 options 節中增加自定的 BIND 版本資訊，可隱藏 BIND 服務器的真正版本號
例如：`version "guess what?";`
此時如果通過 DNS 服務查詢 BIND 版本資訊時，傳回的資訊就是"guess what?"
- 要禁止 DNS 域名遞迴查詢，在 options (或特定的 zone 區域) 節中增加：
`recursion no;`

fetch-glue no;

另一個方法為在啟動 named 時加上 `-r` 參數，即可關閉遞迴查詢。

- 要增加查詢請求 ID 值的隨機性，在 options 節中增加：

use-id-pool yes;

則伺服器將亂數產生 ID 值以避免出現重複。注意這將會使伺服器多占用超過 128KB 記憶體。

- 要限制對 DNS 伺服器做域名查詢的主電腦，可增加 `allow-query{}` 的設定。
- 要限制對 DNS 伺服器做遞迴查詢的主電腦，可增加 `allow-recursion{}` 的設定。
- 要限制哪些主電腦可對 DNS 伺服器做資料的動態更新，可增加 `allow-update{}` 的設定。
- 要限制哪些主電腦可對 DNS 伺服器做 zone transfer 的動作，可增加 `allow-transfer{}` 的設定。
- 要指定不接受哪些伺服器的 zone transfer 請求，可增加 `blackhole{}` 的設定。
- 其它還有一些資源限制的選項可使用像是：`coredump`、`datasize`、`files`、`max-ixfr-log-size`、`stacksize` 等等，可依照伺服器所在的環境做調整。

6.3 DNSSEC 的使用

在 8.1.x 之後 ISC 就新增了 DNSSEC 的功能，藉由加密 DNS 資料來增加服務的安全性。主加密密鑰用於對第一級域名的加密密鑰進行加密簽字，第一層域名(.com, .tw 等)密鑰用於對自身資料及其子域名密鑰進行加密簽名，以此類推。例如，foo.com 的域名伺服器由.com 域密鑰簽名，foo.com 域密鑰則用於對 www.foo.com 域名進行加密簽名。但是目前使用 DNSSEC 功能的伺服器並不會很多，所以如果你想測試這樣的功能，可以加入相關的群組[6][8]參與他們的實驗計畫。

7. 參考資料

1. BIND 8+ 域名伺服器安全增強 by backend , <http://www.nsfocus.com>.
2. BIND 9 域名伺服器更安全(一) by wuming (<mailto:wuming@geekbone.org>), <http://geekbone.org>.
3. CERT® Advisory CA-2001-02 Multiple Vulnerabilities in BIND, <http://www.cert.org/advisories/CA-2001-02.html>
4. CERT® Advisory CA-1999-14 Multiple Vulnerabilities in BIND, <http://www.cert.org/advisories/CA-1999-14.html>
5. CERT* Advisory CA-98.05, http://www.cert.org/advisories/CA-98.05.bind_problems.html
6. Domain Name System Security, <http://www.toad.com/~dnssec/>.
7. DNS Security in Australia, Adrian Ashbury and Craig S Wright, DeMorgan, June 2000.
8. FMESH/CAIRN DNS Key Management Home Page, <https://keys.cairn.net/>.

9. Lion Worm Analysis Version 0.12, <http://www.sans.org/y2k/lion.htm>, April 18, 2001.