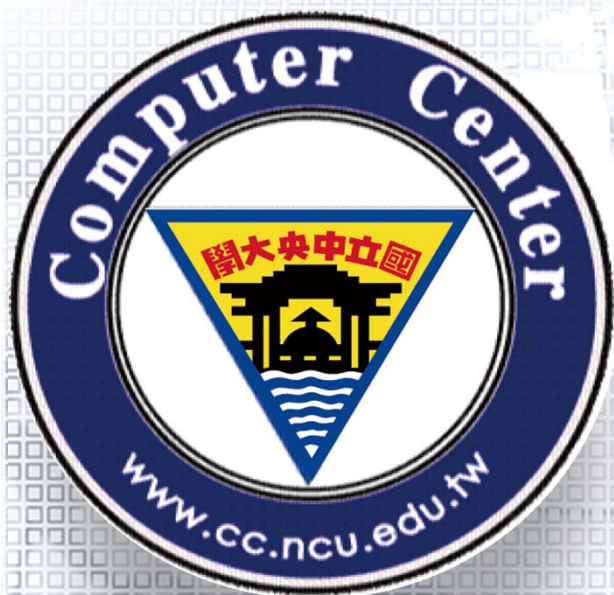


桃園區網中心 第60次區網會議

國立中央大學電算中心
106年12月07日



DNS bind 版本升級 及 新版弱點掃描平台簡介

國立中央大學電算中心
邱惠隆

106年12月07日



DNS bind 版本升級

- 在2016年，BIND曾經出現過兩次漏洞。綠盟科技發佈ISC BIND 9 DoS漏洞技術分析與防護方案，BIND9 DoS漏洞CVE-2016-8864 綠盟科技發佈技術分析與防護方案。
- 106年4月13日，互聯網系統協會（ISC）又發佈了DNS軟體BIND更新，修復了可遠端利用的數個拒絕服務漏洞。
- BIND 9.9.9-P8、9.10.4-P8和9.11.0-P5中修復了可導致聲明失敗的三個安全性漏洞。
- **三個漏洞中CVE-2017-3137為高風險漏洞**

資料來源參考<https://twcertcc.org.tw/twcert/news/10>



DNS bind 版本升級(續)

漏洞描述如下：

CVE ID	威脅程度	攻擊方式	描述
CVE-2017-3136	中	遠程	使用了設置 "break-dnses" 參數為 "yes" 的DNS64在處理生成的畸形DNS記錄時導致拒絕服務。
CVE-2017-3137	高	遠程	伺服器處理一個包含CNAME或者DNAME的畸形回應包時，導致解析器終止，造成拒絕服務。
CVE-2017-3138	中	遠程	允許發送命令的主機在控制通道上發送空命令字串，會導致後臺解析服務程式因為REQUIRE異常而退出。

資料來源參考<http://blog.nsfocus.net/isc-bind-9-multiple-remote-denial-service-vulnerability/>



DNS bind 版本升級(續)

受影響的版本

- CVE-2017-3136影響的版本：

BIND 9 Version 9.8.0 -> 9.8.8-P1
BIND 9 Version 9.9.0 -> 9.9.9-P6
BIND 9 Version 9.9.10b1->9.9.10rc1
BIND 9 Version 9.10.0 -> 9.10.4-P6
BIND 9 Version 9.10.5b1->9.10.5rc1
BIND 9 Version 9.11.0 -> 9.11.0-P3
BIND 9 Version 9.11.1b1->9.11.1rc1
BIND 9 Version 9.9.3-S1 -> 9.9.9-S8

- CVE-2017-3138影響的版本：

BIND 9 Version 9.9.9->9.9.9-P7
BIND 9 Version 9.9.10b1->9.9.10rc2
BIND 9 Version 9.10.4->9.10.4-P7
BIND 9 Version 9.10.5b1->9.10.5rc2
BIND 9 Version 9.11.0->9.11.0-P4
BIND 9 Version 9.11.1b1->9.11.1rc2
BIND 9 Version 9.9.9-S1->9.9.9-S9

- CVE-2017-3137影響的版本：

BIND 9 Version 9.9.9-P6
BIND 9 Version 9.9.10b1->9.9.10rc1
BIND 9 Version 9.10.4-P6
BIND 9 Version 9.10.5b1->9.10.5rc1
BIND 9 Version 9.11.0-P3
BIND 9 Version 9.11.1b1->9.11.1rc1
BIND 9 Version 9.9.9-S8

資料來源參考<http://blog.nsfocus.net/isc-bind-9-multiple-remote-denial-service-vulnerability/>



DNS bind 版本升級(續)

升級過程(以centOS 7.x為例)

先到 <http://www.isc.org/downloads/> 下載新版本軟體 ftp至home目錄

```
#tar -xvf bind-XX.XX.XX.tar.gz (新版本) (解壓縮下載下來的新版本)
#cd bind-XX.XX.XX (解壓縮完後到新版本的目錄)
#./configure --enable-ipv6 --enable-threads --enable-rrl (以一般 user身分)
#sudo -s
#make
#/usr/local/sbin/named -Version (此時應是BIND NN.NN.NN)(舊版本)
#make install
#ls -al /usr/local/sbin/named
#/usr/local/sbin/named -Version (此時應是BIND XX.XX.XX ;新版本)
#ps -ax|grep named
#kill -9 xxx
#/usr/local/sbin/named -c /etc/named.conf -u named
#ps -ax|grep named
#rndc status
#chown named /var/named
#systemctl restart named (再重啟named)
```



DNS bind 版本升級(續)

如何避免版本被查詢

只要在 **/etc/named.conf** 裡增加一行 `version "xxxxxxx"` ;留空或 **Security!!** 之類的文字然後重新啟動 `named` 或是重讀設定檔 就可以了。

```
options {  
directory "/var/named";  
(略)  
version "xxxxx";  
(略)
```

- 這樣修改後，就不會呈現真的 bind 版本，而是呈現你設定的文字。



新版弱點掃描平台簡介

計畫單位：

- 成大電機系網際網路實驗室

計畫名稱：

- 教育單位網站資安弱點掃描防護服務計畫

使用對象：

- 區網中心、縣市網中心及轄下連線單位
- 帳號密碼由計畫單位派發(區網中心向計畫單位申請後由區網中心派發給連線單位)
- 正式上線時間:未知(目前測試中)



新版弱點掃描平台簡介(續)

使用網域:

- 中心單位：依初登入所填網域來新增網站
- 轄下單位：依轄下單位初登入所填網域；若轄下單位未填網域(如:尚未完成初登入帳號)則依管理者網域驗證

使用IP:僅限區網中心及縣市網中心

- 若轄下單位欲使用IP需由中心協助以「匯入」方式處理

匯入格式請由系統下載範本填寫後上傳

- 欄位：單位代碼、主機網域、用途
- 工作表名稱：檢測目標



新版弱點掃描平台簡介(續)

- 因弱掃主機資源有限，需限制檢測數量(未來視情況調整)
 - 區網中心、縣市網中心：5個
 - 轄下單位：2個
- 排程日期
 - 可供排程的時段:每日開放3天後~30天內的日期
 - 週一~五，每日有2種時段：
 - 晚間時段(17~24點)：3個檢測上限
 - 凌晨時段(0~8點)：5個檢測上限
 - 申請：單網站：可選擇排程日期
 - 多網站：由系統自動排程
- 排程日期僅為排程參考依據，實際掃描時間需視掃描狀況而定
- 限制：
 - 非edu網域，無法納入弱掃的新增轄下單位（雖然是連線單位），也不可代為掃描。
 - 無單位代碼的edu網域，處理方式：由區縣網中心使用IP方式新增目標(網站)，代為申請掃描，完成後，報告會轉交給申請單位。



新版弱點掃描平台簡介(續)

- 預計明年安排一場教育訓練課程
 - 詳細日期時間會再公佈



工商廣告宣導

□ 網管通訊錄更新

- 若單位名稱、網管人員及聯絡方式有變動請與區網聯絡更新。

□ 教育訓練/講座/會議

- 原則上都安排在星期四

區網連絡人：

邱惠隆

center38@cc.ncu.edu.tw

03-4227151#57516

□ 校園資安推廣

- 推廣對象：教職員及學生均可
- 徵求連線單位講師支援(具有資安相關證照及相關研究)



Computer Center, National Central University.



感謝你的耐心聆聽!

Q&A