# Chargen Service DoS attack

## 分析&解決方案



北區 ASOC 團隊製

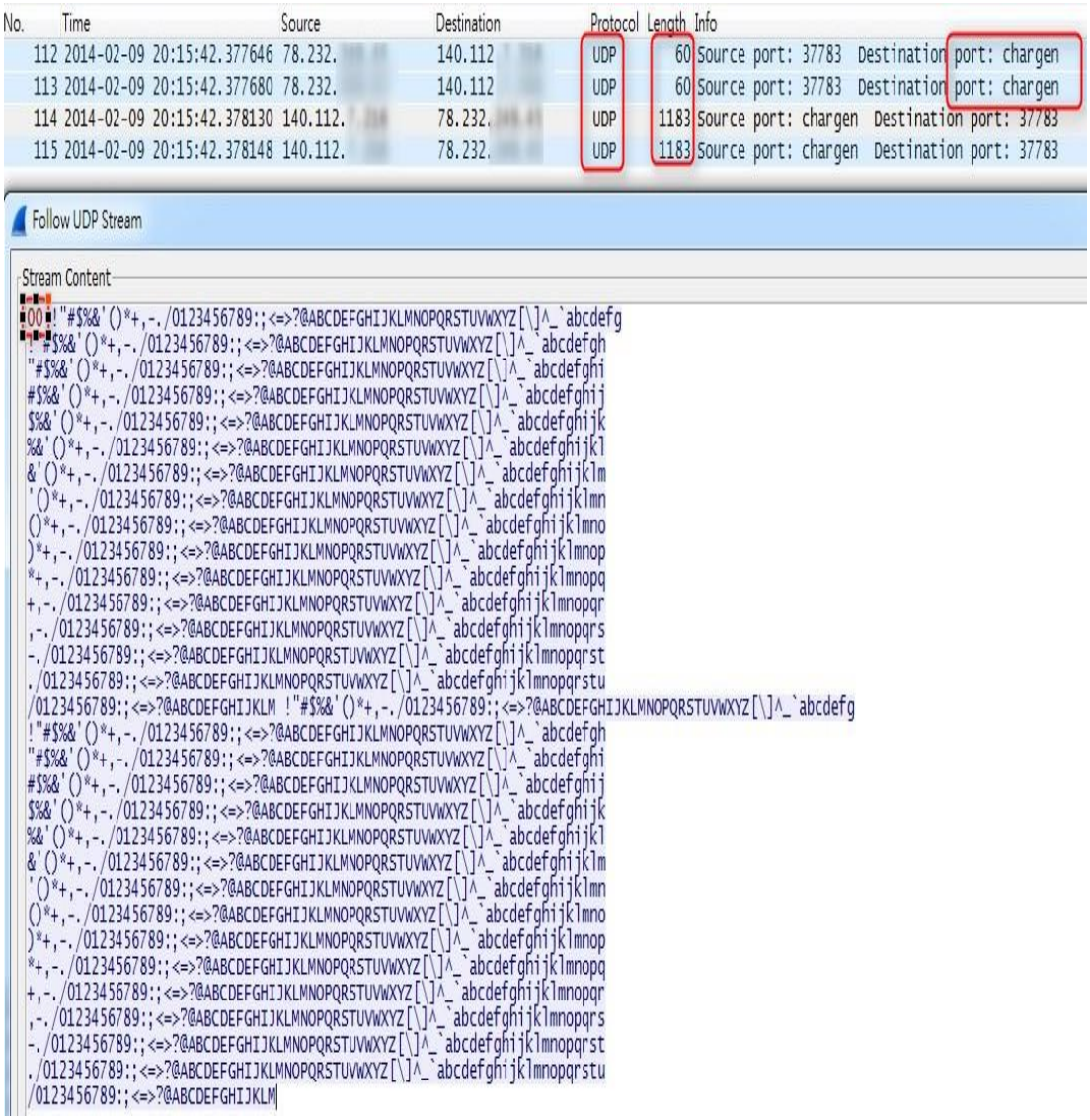
*2014/03*

## 1. Chargen Service DoS attack 簡介

Chargen 協定全名為 Character Generator Protocol，中文為字元符號產生協定。預設通訊 port TCP 19 以及 UDP 19(*於 RFC 864 中定義*)，若透過 TCP port 19 來連結，則 Server 端會不斷回傳任意字串到 Client，直到連線結束。若改採 UDP port 19 進行連線，則 Server 端會重新產生帶有一長串字串的封包檔給 Client 端。此服務主要用途是利用這些網路流量，測試兩台主機間的網路連線或網路頻寬。

但未經完善管理且提供這些服務的設備，非常容易被外部攻擊者利用而發動 DoS 攻擊，攻擊者通常利用 UDP 連線方式，向 server 端發送偽造來源 IP 位址的封包，而提供此服務的 server，向受害主機不斷傳送含有亂數字元的封包，此攻擊亦具有流量放大的效果。從臺灣大學所發現的實際案例中，可以看到攻擊者所傳送的封包長度僅 60byte，而 Server 端回傳之封包長度達 1183byte，流量被放大了將近 20 倍，所產生的 UDP flow 可能會影響正常網路環境運作。

## *透過 UDP 協定的 Chargen 放大攻擊*



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 112 | 2014-02-09 20:15:42.377646 | 78.232. | 140.112 | UDP | 60 | Source port: 37783 Destination port: chargen |
| 113 | 2014-02-09 20:15:42.377680 | 78.232. | 140.112 | UDP | 60 | Source port: 37783 Destination port: chargen |
| 114 | 2014-02-09 20:15:42.378130 | 140.112. | 78.232. | UDP | 1183 | Source port: chargen Destination port: 37783 |
| 115 | 2014-02-09 20:15:42.378148 | 140.112. | 78.232. | UDP | 1183 | Source port: chargen Destination port: 37783 |

Follow UDP Stream

Stream Content

```
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefg
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefgh
"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghij
$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijk
%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklm
'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmn
()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmno
)*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnop
*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopq
+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqr
,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrs
-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrst
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstu
/0123456789:;<=>?@ABCDEFGHIJKLM !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefg
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefgh
"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghij
$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijk
%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklm
'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmn
()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmno
)*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnop
*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopq
+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqr
,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrs
-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrst
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstu
/0123456789:;<=>?@ABCDEFGHIJKLM
```

## 2. Chargen Service DoS attack 解決方案

要徹底解決 Chargen Service DoS attack，建議將主機之該項服務關閉，以下提供不同作業系統的解決方案。

### A. Unix:

1. 編輯/etc/inetd.conf (或相同功能)檔案
2. 尋找 Chargen Service 名稱
3. 於 Chargen Service 服務名稱前，加入”#”，將該指令修改為註解後，該服務將不會被執行
4. 重新啟動 inetd

### B. Windows

1. 開始 > 執行 > 輸入”regedit”，來開啟 Registry editor
2. 尋找註冊碼位置

   *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SimpTcp\Parameters.*
3. 雙擊” EnableTcpChargen”註冊碼選項，並將其值修改為”0”(DWORD)
4. 雙擊” EnableUdpChargen”註冊碼選項，並將其值修改為”0”(DWORD)
5. 重新啟動 TCP/IP 連線

### C. Novell:

1. 安裝 NIAS4.0 或更高版本

2. 載入 INETCFG > Protocols > TCP/IP ，並將”set filter support”開啟
3. 載入 FILTCFG > TCP/IP > Packet Forwarding filters，並將其設置為”開啟”
4. 編輯封包過濾器清單，並點擊 ENTER 進入編輯
5. 點擊”INSERT”並選擇封包類型為:Name:<all>
6. 輸入 ENTER 後，尋找 chargen service port:Port 19
7. 輸入 ENTER 後，離開並儲存 Filters 設置選擇:YES


# 北區學術資訊安全維運中心