

臺灣大學計資中心網路組 北區學術資訊安全維運中心 資訊安全分析報告

Ð

資訊

Chargen Service DoS attack

學術資

NTU-ASOC

分析&解決方案

北區 ASOC 團隊製

2014/03



2.

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 por	rt: 37783	Destination	n port: char	rgen
	113	2014-02-09	20:15:42.377680	78.232.	140.112	UDP	60	Source por	rt: 37783	Destination	n port: char	rgen
	114	2014-02-09	20:15:42.378130	140.112.	78.232.	UDP	1183	Source por	rt: charge	n Destinat	ion port: 3	7783
	115	2014-02-09	20:15:42.378148	140.112.	78.232.	UDP	1183	Source por	rt: charge	n Destinat	ion port: 3	7783
	_						_		,			
1	Follov	v UDP Stream										
S	tream	Content										
	0011"	#\$%&'()*+.	/0123456789::<	=>?@ABCDEFGHIJKLM	NOPORSTUVWXYZ[\]^ `a	bcdefa						
	#\$%	&'()*+,/	0123456789:;<=>?	@ABCDEFGHIJKLMNOP	QRSTUVWXYZ[\]^_`abcd	efgh						
	#\$%8	()*+,/0	123456789:;<=>?@	ABCDEFGHIJKLMNOPQ	RSTUVWXYZ[\]^_`abcde	fghi						
	₹3%& t%&'(()*+,/01	23456780::<=>?@A 2456780::<=>?@AP		STUVWXYZ[\]^_ abcdef	ghij Gijk						
	68'()	*+/0123	456789::<=>?@ABC	DEFGHIJKLMNOPORST	UVWXYZ[\]^ `abcdefgh	iik]						
	§'()*	+,/01234	56789:;<=>?@ABCD	EFGHIJKLMNOPQRSTU	vwxYZ[\]^_`abcdefghi	jklm						
	'()*+	,/012345	6789:;<=>?@ABCDE	FGHIJKLMNOPQRSTUV	wxyz[\]^_`abcdefghij	<u>ƙ</u> 1mn						
	()*+,	/0123456	789:;<=>?@ABCDEF	GHIJKLMNOPQRSTUVW	XYZ[\]^_ abcdefghijk	Imno						
)°+,- *+ -	/012345678	09:;<=>?@ABCDEFG 9::<=>?@ABCDEFGH	IT TKLMNOPQRSTUVWA	72[\]∧_`abcdefghiik]m	nong						
	+/	0123456789	::<=>?@ABCDEFGHI	JKLMNOPQRSTUVWXYZ	[\]^_`abcdefghijklmn	opar						
	,/0	123456789:	;<=>?@ABCDEFGHIJ	KLMNOPQRSTUVWXYZ [<pre>\]^_`abcdefghijk1mno</pre>	pars						
	/01	23456789:;	<=>?@ABCDEFGHIJK	LMNOPQRSTUVWXYZ[\]^_`abcdefghijk1mnop	qrst						
	/0123	3430/89:;< 456780··/-	>?@ABCDEFGHIJKL \?@ABCDEEGHTIKLM	MNOPQRSTUVWXYZ[\] 1 !"#\$%&'()*+ = /0	^_ abcdergn1jk1mnopq 123456789∙∙∠=>2@ABCD	EEGHTIKIM	NODODS		A `abcdef	1		
	!"#\$%	&'()*+/	0123456789::<=>?	@ABCDEFGHIJKLMNOP	ORSTUVWXYZ[\]^_`abcd	efah	NUFURS	1040012[\]	- abcder	1		
	"#\$%8	i'()*+,/0	123456789:;<=>?@	ABCDEFGHIJKLMNOPQ	RSTUVWXYZ[\]Ă_`abcde	fghi						
	#\$%&'	()*+,/01	23456789:;<=>?@A	BCDEFGHIJKLMNOPQR	STUVWXYZ[\]^_`abcdef	ghij						
	1%& ()*+,/012	3450/89:;<=>?@AB 456780::<=>?@ABC	CDEFGHIJKLMNOPORS	TUVWXYZ[\]^_ abcdefg	n1]K 1361						
	62 () 8'()*	+,-,/01234	400/09:;<=>?@ABCD 56789::<=>?@ABCD	DEFGHIJKLMNOPORSTU	vwxyz[\]^_ abcdefghi	iklm						
	'()*+	/012345	6789::<=>?@ABCDE	FGHIJKLMNOPQRSTUV	WXYZ[\]^_`abcdefghij	k1mn						
	()*+,	/0123456	789:;<=>?@ABCDEF	GHIJKLMNOPQRSTUVW	xyz[\]^_`abcdefgĥijk	1mno						
)*+,-	./01234567	89:;<=>?@ABCDEFG	HIJKLMNOPQRSTUVWX	YZ[\]^_`abcdefghijkl	mnop						
	*+,	/012345678	9:;<=>?@ABCDEFGH	I JKLMNOPQRSTUVWXY	Z[\]^_ abcdefghijklm	nopq						
	- /0	0123430/89	<pre>:;<=>?@ABCDEFGH1 :/=>?@ABCDEEGH11</pre>	UVWXYZ	\]^_ abcdergnijkimn	nars						
	./01	23456789::	<=>?@ABCDEFGHIJK	(LMNOPORSTUVWXYZ [\	1^`abcdefghiiklmnop	arst						
	/012	3456789:;<	=>?@ABCDEFGHIJKL	MNOPQRSTUVWXYZ [\]	∧_`abcdefghijklmnopq	rstu						
	/0123	456789:;<=	>?@ABCDEFGHIJKLM									
				. 0	- A >			/				

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. 编輯/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

