臺灣大學計資中心網路組
北區資訊安全維運中心

Personal NAS 資安防護

目錄

一、 簡介 Personal NAS 使用原理概述.....3

二、 駭客使用 ShellShock 攻擊 Personal NAS.....3

三、 結論.....6

一、簡介 Personal NAS 使用原理概述

網路附加儲存(Network Attached Storage，NAS)，是一種資料儲存技術的名稱，主要是由一個內嵌的 OS 與數個大容量硬碟所組成，並可經由網路提供其他設備檔案共用的服務，也可以提供使用者資料存取服務。

NAS 系統通常會有一個以上的硬碟，而且和傳統的檔案伺服器一樣，會把所有硬碟組成獨立磁碟備援陣列(Redundant Array of Independent Disk，RAID)提供服務。網路上的其他伺服器可以利用 NAS 進行檔案存取，而不需具備檔案伺服器的功能。

NAS 的優點在於使用者可以直接連結 NAS 進行檔案存取，不需存取其他檔案伺服器，使用者不會因為某些伺服器關閉而無法進行資料存取。NAS 也可以讓資料管理變得更加輕鬆及簡單，讓原本需要在伺服器上進行的繁複設定程序，簡化成幾個安裝步驟就可完成，大大的節省設定的時間與難度。NAS 也讓使用者可建立私人雲端資料存取服務，透過網際網路連線，NAS 可以讓各種裝置在居家或外出時輕鬆進行資料存取。

二、駭客使用 ShellShock 攻擊 Personal NAS

2014 年 9 月，法國的軟體開發人員 Stéphane Chazelas 發佈 Shellshock(CVE-2014-6271)漏洞，這個 Bash Shell 漏洞主要出現在定義的環境變數後面，例如在 Linux 環境下的 Webserver，攻擊者可修改封包的 Header，加上一串 `() { :;};` 的符號字串，利用這個字串可利用系統漏洞，進而對含有 Bash Shell 的系統進行攻擊，可執行符號字串後的任意程式碼，而這類攻擊被稱之為 Shellshock。

利用 Shellshock 的漏洞與 Linux 的語法，在不經過認證的情況下取得攻擊端電腦之權限與資料，駭客甚至可以利用此漏洞執行惡意程式碼或是植入木馬程式。目前駭客利用 Shellshock 攻擊的手法有下列幾種：

1. 攻擊網頁伺服器 CGI
2. 惡意 DHCP 伺服器以感染連線的使用者
3. 繞過 Git 與 Subversion 伺服器的限制進行攻擊

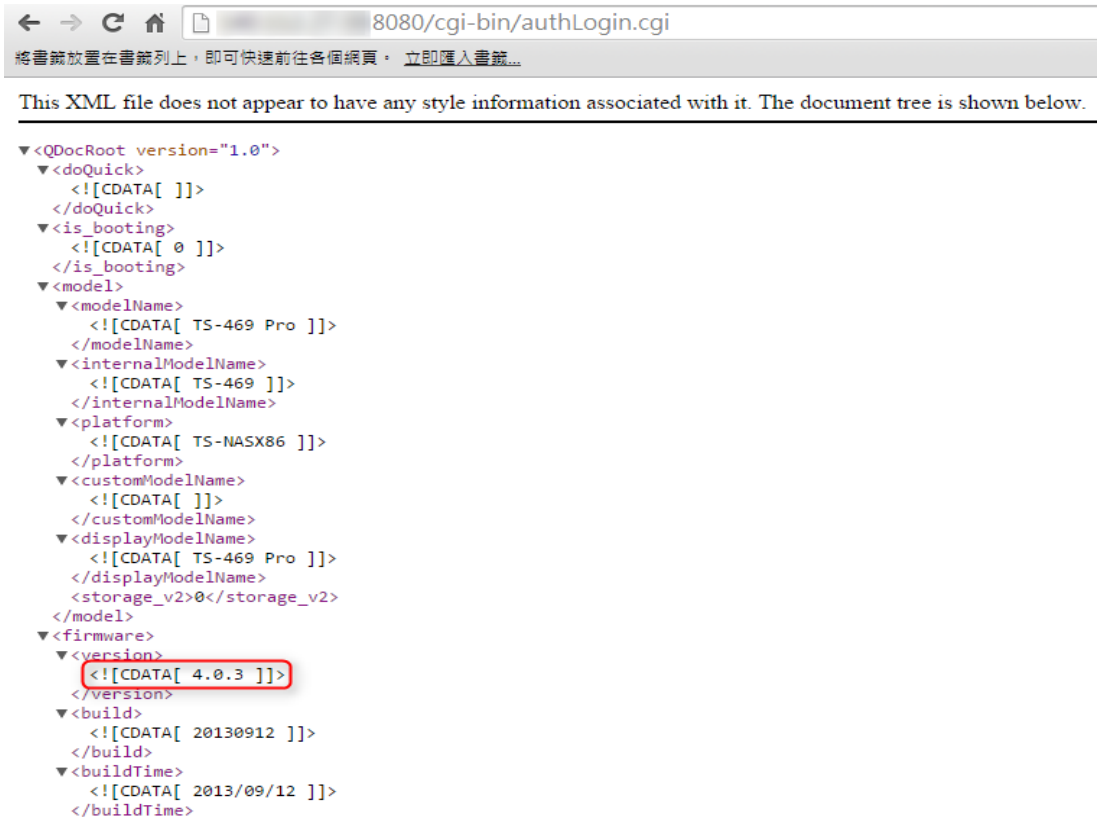
同樣使用 Linux 作業系統的 QNAP 網路儲存裝置(NAS)為例，舊版本存在 Shellshock 漏洞，故可利用前述的攻擊方式，在未經授權的情況下讓 QNAP NAS 執行任意程式碼，以達到竊取資料或攻擊其他目標之目的。

儘管 QNAP 官方在 Shellshock 漏洞出現後釋出修補漏洞的更新程式，但官方統計 2014 年 10 月 5 日全臺仍存在 Shellshock 漏洞的 QNAP NAS 裝置，發現真正有進行更新漏洞的使用者幾乎不到 1 成，也就是說仍有 9 成的 QNAP NAS 仍暴露在風險之中，使得駭客輕易利用該漏洞滲透企業內部網路，進而獲取企業內部資料。接下來，以 QNAP 為範例做為 Shellshock 攻擊流程之說明。

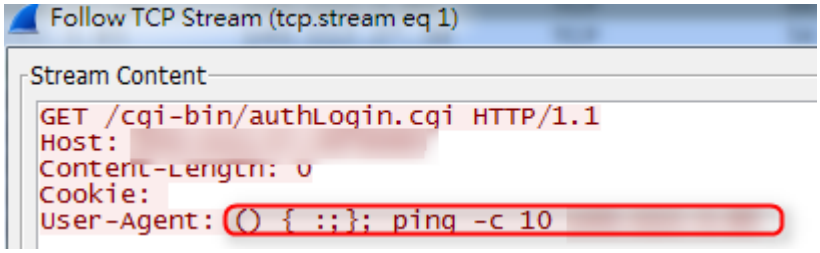
由於 QNAP 的控制頁面同樣為 CGI 網頁伺服器，因此駭客以一些特定條件先掃描 IP 進行過濾。一般來說 QNAP 使用的 Port 為 8080 且為 Apache 網頁伺服器，因此可以利用這兩個規則做為過濾條件進行篩選。

IP	Ports	Hostname	Web detect
[redacted]	80,808	[redacted]	Apache
[redacted]	80,808	[redacted]	Apache
[redacted]	80,808	[redacted]	Apache
[redacted]	80,808	[redacted]	Apache
[redacted]	80,808	[redacted]	Apache
[redacted]	80,808	[redacted]	Apache
[redacted]	80,808	[redacted]	Apache

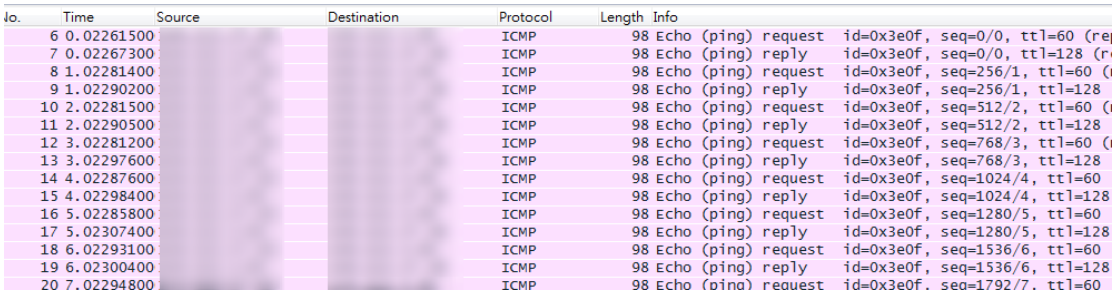
找到可能含有漏洞之 IP 位址，將其 IP 後方加上" :8080/cgi-bin/authLogin.cgi"，接著確認裝置名稱與其系統版本。



尚未更新至 4.1.2 版本之軟體有 Shellshock 漏洞之風險，將指令塞入封包之 HTTP Header 令其 Ping 特定 IP，可以看到在 Ping 指令前面加上一串 () { :;}; 的符號字串以利用系統之漏洞。



在被 Ping 之主機上進行封包側錄，可以發現確實有收到 QNAP 裝置傳來 Ping 的事件封包，代表此裝置確實存在 Shellshock 漏洞。



No.	Time	Source	Destination	Protocol	Length	Info
6	0.02261500	[redacted]	[redacted]	ICMP	98	Echo (ping) request id=0x3e0f, seq=0/0, ttl=60 (re
7	0.02267300	[redacted]	[redacted]	ICMP	98	Echo (ping) reply id=0x3e0f, seq=0/0, ttl=128 (r
8	1.02281400	[redacted]	[redacted]	ICMP	98	Echo (ping) request id=0x3e0f, seq=256/1, ttl=60 (
9	1.02290200	[redacted]	[redacted]	ICMP	98	Echo (ping) reply id=0x3e0f, seq=256/1, ttl=128
10	2.02281500	[redacted]	[redacted]	ICMP	98	Echo (ping) request id=0x3e0f, seq=512/2, ttl=60 (
11	2.02290500	[redacted]	[redacted]	ICMP	98	Echo (ping) reply id=0x3e0f, seq=512/2, ttl=128
12	3.02281200	[redacted]	[redacted]	ICMP	98	Echo (ping) request id=0x3e0f, seq=768/3, ttl=60 (
13	3.02297600	[redacted]	[redacted]	ICMP	98	Echo (ping) reply id=0x3e0f, seq=768/3, ttl=128
14	4.02287600	[redacted]	[redacted]	ICMP	98	Echo (ping) request id=0x3e0f, seq=1024/4, ttl=60
15	4.02298400	[redacted]	[redacted]	ICMP	98	Echo (ping) reply id=0x3e0f, seq=1024/4, ttl=128
16	5.02285800	[redacted]	[redacted]	ICMP	98	Echo (ping) request id=0x3e0f, seq=1280/5, ttl=60
17	5.02307400	[redacted]	[redacted]	ICMP	98	Echo (ping) reply id=0x3e0f, seq=1280/5, ttl=128
18	6.02293100	[redacted]	[redacted]	ICMP	98	Echo (ping) request id=0x3e0f, seq=1536/6, ttl=60
19	6.02300400	[redacted]	[redacted]	ICMP	98	Echo (ping) reply id=0x3e0f, seq=1536/6, ttl=128
20	7.02294800	[redacted]	[redacted]	ICMP	98	Echo (ping) request id=0x3e0f, seq=1792/7, ttl=60

三、結論

Shellshock 漏洞主要的攻擊目標是含有 bash 的 Linux 系統，因此受害範圍相當廣泛，但並非含有漏洞的 bash 版本就會遭受攻擊，要成功的執行 Shellshock 攻擊依然需要許多其他的條件，目前較需要注意的設備或伺服器如下：

- 特定 Linux 版本，並且使用 DHCP 連線
- 網路、資安設備
- 使用 CGI 的網站伺服器
- 已經公布含有弱點的套件

當發生 Shellshock 漏洞的攻擊時，應儘速將 Bash 升級至最新版本以修補該漏洞，尤其是針對使用含有漏洞版本的 Bash 之 Linux 設備，如 QNAP 更新至 4.1.2 便可修補該漏洞。若是屬於規模較大的單位，則以設備重要性之優先順序進行更新。

此外，學校可使用入侵防禦系統(IPS)、網站應用程式防火牆(WAF)等防禦設備阻擋 Shellshock 攻擊，評估是否停用安全性較低的 CGI 伺服器機制，改用其它替代方案，另可以強化使用 Linux 系統之伺服器的資安等級，如使用增強安全性的 SELinux 或 AppArmor 等。

Shellshock 影響相當廣泛，各廠商也推出新的系統更新以解決此漏洞，只要將伺服器 bash 版本升級至最新版本，並持續關注官方後續更新訊息，定期檢查企業使用網路設備是否在各家廠商系統更新名單內，及早發現修補更新設備，便可防堵此漏洞。

參考資料：

CVE-2014-6271 - NVD – Detail，網址:
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271

Shaolinon(2014)，Shellshock (Bash CVE-2014-6271) 威脅仍在擴大中，但無需過度恐慌，網址: http://devco.re/blog/2014/09/30/shellshock-CVE-2014-6271/

Shellshock (software bug) - Wikipedia, the free encyclopedia，網址:
http://en.wikipedia.org/wiki/Shellshock_(software_bug)

余至浩(2014)，雅虎遭駭！Shellshock 出現首宗大型網站災情，網址:
http://www.ithome.com.tw/news/91432