# 國家資通安全會報 行政院國家資通安全會報技術服務中心

# 漏洞/資安訊息警訊

| | | | |
|---|---|---|---|
| 發布編號 | NCCST-ANA-2016-0085 | 發布時間 | Fri Aug 26 18:16:09 CST 2016 |
| 事件類型 | 漏洞預警 | 發現時間 | Fri Aug 19 00:00:00 CST 2016 |
| 警訊名稱 | Cisco 與 Fortinet 防火牆產品存在多個安全漏洞，部分漏洞允許攻擊者以管理者權限進行遠端存取或執行任意程式碼 | | |
| 內容說明 | 2016 年 8 月 15 日，國際上名為影子掮客(The Shadow Brokers)的駭客團體，公開販售及釋出多款網路攻擊工具，影響 Cisco 與 Fortinet 等多款防火牆設備，部分漏洞允許攻擊者以管理者權限進行遠端存取或執行任意程式碼，漏洞說明如下：<br><br>1. Cisco<br><br>Cisco Adaptive Security Appliances(ASA)軟體是美國 Cisco 公司所開發的一套運行在防火牆中的操作系統，目前已知受影響的相關漏洞編號為 CVE-2016-6366 與 CVE-2016-6367。<br><br>(1) CVE-2016-6366 漏洞<br><br>主要是 ASA 軟體在 9.4.2.3(含)之前版本的 SNMP 程式碼存在緩衝區溢位漏洞(Buffer overflow)，當遠端攻擊者發送特製的 SNMP 封包到受影響的系統上，就能造成重載(Reload)作業系統或遠端執行任意程式碼，甚至取得系統的控制權限。<br><br>(2) CVE-2016-6367 漏洞<br><br>ASA 軟體 8.4(1)之前版本的 Command-line Interface(CLI)語法分析器(Parser)存在安全漏洞，該漏洞可讓本地端未經身分驗證的攻擊者在受影響的設備上，調用(Invoking)某些特定無效的命令造成阻斷服務攻擊(DoS)，或是執行任意程式碼。 | | |

| | |
|---|---|
| | 2. Fortinet<br><br>FortiGate 防火牆是美國 Fortinet 公司生產的防火牆設備，FortiGate 韌體版本為 4.3.8、4.2.12、4.1.10(含)之前的防火牆設備存在緩衝區溢位漏洞(Buffer overflow)，當攻擊者發送特製的 HTTP 封包請求時，由於程式未能對攻擊者輸入的內容長度執行正確的檢查，造成攻擊者可利用此漏洞以管理者權限進行遠端存取或執行任意程式碼。<br><br>請各機關檢視防火牆設備是否採用受影響之軟體或韌體版本，並儘速更新至最新版本。 |
| 影響平台 | 1.Cisco 已知受影響 ASA 軟體版本：<br><br>(1)ASA 8.7(含)版以下。<br><br>(2)ASA 9.4.2.3(含)版以下。<br><br>Cisco 已知受影響設備如下：<br><br>(3)Cisco ASA 5500 Series Adaptive Security Appliances。<br><br>(4)Cisco ASA 5500-X Series Next-Generation Firewalls。<br><br>(5)Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers。<br><br>(6)Cisco ASA 1000V Cloud Firewall。<br><br>(7)Cisco Adaptive Security Virtual Appliance (ASAv) 。<br><br>(8)Cisco Firepower 4100 Series。<br><br>(9)Cisco Firepower 9300 ASA Security Module。<br><br>(10)Cisco Firepower Threat Defense Software。<br><br>(11)Cisco Firewall Services Module (FWSM)。<br><br>(12)Cisco Industrial Security Appliance 3000。<br><br>(13)Cisco PIX Firewalls。 |

| | |
|---|---|
| | 2.FortiGate 已知受影響韌體版本如下：<br><br>(1)FortiGate 4.3.8(含)版以下。<br><br>(2)FortiGate 4.2.12(含)版以下。<br><br>(3)FortiGate 4.1.10(含)版以下。 |
| 影響等級 | 高 |
| 建議措施 | 請各機關聯絡設備維護廠商或原廠確認防火牆設備所採用之 ASA 版本或 FortiGate 韌體版本，若使用版本為受影響之 ASA 版本或 FortiGate 韌體版本，則請參考以下建議修復資訊：<br><br>1.針對漏洞為 CVE-2016-6366 之漏洞：<br><br>(1)ASA 8.7(含)之前版本，請更新至 9.1.7(9)或更高的版本。<br><br>(2)ASA 9.0 版本，請更新至 9.0.4(40)版本。<br><br>(3)ASA 9.1 版本，請更新至 9.1.7(9)版本。<br><br>(4)ASA 9.2 版本，請更新至 9.2.4(14)版本。<br><br>(5)ASA 9.3 版本，請更新至 9.3.3(10)版本。<br><br>(6)ASA 9.4 版本，請更新至 9.4.3(8)版本。<br><br>2.針對漏洞為 CVE-2016-6367 之漏洞<br><br>(1)ASA 8.4(含)之前的版本，請更新至 8.4(3)或更高的版本。<br><br>(2)ASA 8.5~9.0(含)之間的版本，請更新至 9.0(1)或更高的版本。<br><br>3.針對 FortiGate 韌體為 4.3.8、4.2.12、4.1.10(含)之前的版本，則請更新至 5.x 版本，若設備無法相容 5.x 版本，請至少升級至 4.3.9(含)以上的版本。<br><br>4.其它建議事項：<br><br>(1)其餘未列在上述修復資訊之 ASA 版本，請密切注意 Cisco 官方網頁(https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp 與 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-cli)之更新資訊。 |

| | |
|---|---|
| | (2)Cisco Firewall Services Module (FWSM)與 Cisco PIX Firewalls 設備，因產品過舊，目前已無相關的修復程式。 |
| 參考資料 | 1.http://fortiguard.com/advisory/FG-IR-16-023<br><br>2.http://thehackernews.com/2016/08/nsa-hack-exploit.html<br><br>3.http://thehackernews.com/2016/08/nsa-hack-russia-leak.html<br><br>4.https://cxsecurity.com/cveshow/CVE-2016-6366/<br><br>5.http://www.ithome.com.tw/news/107916<br><br>6.http://www.ithome.com.tw/news/107826 |

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw