Cisco 與 Fortinet 等多款防火牆設備存在數個安全漏洞，部分漏洞允許攻擊者遠端取得設備控制權或遠端執行任意程式碼

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，且部分漏洞允許攻擊者遠端取得設備控制權或遠端執行任意程式碼。

目前廠商已確認之漏洞與受影響設備如下：

1. Cisco

(1)CVE-2016-6366 漏洞之受影響設備包含：

-Cisco ASA 5500 Series Adaptive Security Appliances

-Cisco ASA 5500-X Series Next-Generation Firewalls

-Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers

-Cisco ASA 1000V Cloud Firewall

-Cisco Adaptive Security Virtual Appliance (ASAv)

-Cisco Firepower 4100 Series

-Cisco Firepower 9300 ASA Security Module

-Cisco Firepower Threat Defense Software

-Cisco Firewall Services Module (FWSM)

-Cisco Industrial Security Appliance 3000

-Cisco PIX Firewalls

(2)CVE-2016-6367 漏洞之受影響設備包含：

-Cisco ASA 5500 Series Adaptive Security Appliances

-Cisco ASA 5500-X Series Next-Generation Firewalls

-Cisco PIX Firewalls

-Cisco Firewall Services Module (FWSM)

2. Fortinet

緩衝區溢位漏洞之受影響設備包含韌體為 4.3.8(含)之前的版本，包含：

-FortiGate 4.3.8(含)版以下

-FortiGate 4.2.12(含)版以下

-FortiGate 4.1.10(含)版以下

影響平台：

多款 Cisco、Fortinet 等防火牆設備

建議措施：

目前僅有部分廠商確認相關漏洞與受影響設備範圍，因此建議隨時提高警覺，以降低資安威脅，以下列出已知之修補建議供參考：

1.針對編號為 CVE-2016-6367 之漏洞，若採用的 Cisco 設備為 ASA 8.4(含)之前的版本，請更新至 8.4(3)或更高的版本；採用 ASA 9.0(含)之前的版本，則請更新至 9.0(1)或更高的版本。

2.針對編號為 CVE-2016-6366 之漏洞，目前 Cisco 官方尚無釋出正式的修復版本，故仍請密切注意 Cisco 官方網頁(https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp)之更新訊息。

Fortinet 相關防火牆設備，則請將受影響之 FortiGate 韌體升級至 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。

參考資料：

http://thehackernews.com/2016/08/nsa-hack-exploit.html
http://thehackernews.com/2016/08/nsa-hack-russia-leak.html
https://tools.cisco.com/security/center/publicationListing.x?product=NonCisco#~Vulnerabilities
http://www.ithome.com.tw/news/107780
http://hk.thenewslens.com/article/47062
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-cli
https://fortiguard.com/advisory/FG-IR-16-023

Publish Date

2016/8/24 0:00:00