From: 國家資通安全會報技術服務中心
Sent: Friday, January 15, 2016 5:15 PM
To: ncert@icst.org.tw
Subject: [資安訊息警訊] 國家資通安全會報技術服務中心(事件編號：ICST-ANA-2016-0009)

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	ICST-ANA-2016-0009	發布時間	Fri Jan 15 16:14:59 CST 2016
事件類型	漏洞預警	發現時間	Thu Jan 14 00:00:00 CST 2016
警訊名稱	特定版本 Fortigate 防火牆存在 SSH 認證管理漏洞，請儘速確認並更新版本		
內容說明	Fortinet 的 Fortigate 防火牆存在 SSH 的認證管理漏洞，所有搭載 FortiOS 版本 4.3.0 至 4.3.16，以及版本 5.0.0 至 5.0.7 的防火牆，攻擊者可透過 SSH 連線，利用特定的帳號與密碼存取相關設備。 可使用以下兩種方法查詢 Fortigate 版本資訊： 1.Web 網頁介面 以 Fortigate 111C 為例，以 admin 身分登入系統後，點選左側 Dashboard -> Status，即可檢視設備版號(如附件一)，圖為 FortiOS v5.0.2。 2.從 CLI 介面取得 以 Fortigate-50B 為例，進入設備 CLi 介面，輸入指令 get sys status 取得設備資訊，即可檢視設備版號(如附件二)，圖為 FortiOS v4.3.7。 請各機關檢視所支援的 FortiOS 版本，若版本為「Fortios 4.3.0 至 4.3.16」或「Fortios 5.0.0 至 5.0.7」，請儘速針對存在已知弱點進行修正，並檢視防火牆 SSH 登入紀錄，確認無異常登入情況。		
影響平台	1.Fortios 4.3.0 至 4.3.16 2.Fortios 5.0.0 至 5.0.7		

影響等級	高
建議措施	1.Fortios4.3.X 建議更新至 4.3.17 以上或最新版本、Fortios5.0.X 建議更新至 5.0.8 以上或最新版本。 2.建議關閉 SSH 功能，僅以 Web 管理介面進行調整。 3.如需要以 SSH 連線方式管理，建議除了更新版本外，另限制最小 IP 範圍能連線至設備。
參考資料	1.http://www.fortiguard.com/advisory/fortios-ssh-undocumented-interactive-login-vulnerability 2.http://blog.fortinet.com/post/brief-statement-regarding-issues-found-with-fortios 3.http://news.softpedia.com/news/ssh-backdoor-identified-in-fortinet-firewalls-498816.shtml 4.http://seclists.org/fulldisclosure/2016/Jan/26 5.http://thehackernews.com/2016/01/fortinet-firewall-password-hack.html

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。國家資通安全會報 技術服務中心 (http://www.icst.org.tw/)

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@icst.org.tw