張貼日期：2016/01/19

轉發漏洞/資安訊息警訊

主旨：【漏洞預警】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

說明：

- 轉發國家資通安全會報 技術服務中心 漏洞/資安訊息警訊 ICST-ANA-201601-0022
  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

  附件下載位址：http://cert.tanet.edu.tw/download/Fortigate.rar

  請檢視所支援的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

- [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

---

計算機與通訊中心
網路系統組 敬啟

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20160119_01

Last update: **2016/01/21 15:43**