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-2018-0097	發布時間	Mon Oct 15 10:01:39 CST 2018
事件類型	漏洞預警	發現時間	Fri Oct 12 00:00:00 CST 2018
警訊名稱	Juniper NFX 系列之 Junos OS 18.1 版本存在安全漏洞(CVE-2018-0044)，允許攻擊者遠端登入，請儘速確認並進行修正		
內容說明	Juniper Junos OS 是 Juniper Networks 公司一套以 FreeBSD 為基礎所發展，專用於該公司網路設備的作業系統。 研究人員發現 Juniper NFX 系列之 Juniper 裝置管理員(Juniper Device Manager，簡稱 JDM)與作業系統存在 CVE-2018-0044 安全漏洞，肇因於 sshd 預設將「PermitEmptyPasswords」選項設定為「yes」，當網路設備存在密碼設為空白之使用者帳號時，攻擊者可藉由猜測帳號並使用空白密碼嘗試進行遠端登入。		
影響平台	Juniper NFX 系列之 Junos OS 18.1 至 18.1R4 以前版本		
影響等級	高		
建議措施	目前 Juniper 官方已針對此弱點釋出修復版本，請各機關可聯絡設備維護廠商或參考以下建議進行更新： 1.於 Juniper NFX 系列網路設備之指令介面輸入「show version」指令確認當前使用的版本。 2.如使用受影響之 Junos OS 版本，請瀏覽 Juniper 官方下載網頁(https://support.juniper.net/support/downloads/)，將版本升級至 18.1R4 或 18.2R1。 3.若無法立即更新，可進行下列替代措施： (1)請確認 JDM 與 Junos OS 中所有使用者帳號皆有設定密碼。 (2)請將 JDM 與 Junos OS 之/etc/ssh/sshd_config 檔案中的「PermitEmptyPasswords」選項設為「no」。		
參考資料	1. https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10878&actp=		

	METADATA 2. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0044 3. https://www.ithome.com.tw/news/126377

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