

張貼日期：2018/10/15

[資安漏洞預警通知] 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

主旨：[資安漏洞預警通知] 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。

- 影響平臺：Juniper NFX系列之Junos OS 18.1至18.1R4以前版本

- 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>

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:20181015_01

Last update: 2018/10/15 15:33