

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-2018-0096	發布時間	Mon Oct 15 10:01:48 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 Junos OS 之 NTP 套件存在多個安全漏洞，允許攻擊者遠端執行任意程式碼，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。 Juniper 官方於 10 月份的安全建議與警訊中，公告 Junos OS 之 NTP 套件存在多個安全漏洞，其中又以 CVE-2018-7183 最為嚴重，當攻擊者針對使用 Junos OS 的網路設備進行 NTP 功能查詢時，藉由發送特製的惡意封包可使其 decodearr 函數出現緩衝區溢位情況，導致攻擊者可遠端執行任意程式碼。		
影響平台	所有使用 Junos OS 的網路設備，包含： · J 系列 · M 系列 · T 系列 · MX 系列 · EX 系列 · SRX 系列 · QFX 系列 · NFX 系列 · PTX 系列		
影響等級	高		

目前 Juniper 官方已針對弱點釋出修復版本，請各機關可聯絡設備維護廠商將 Junos OS 升級至以下版本：

建議措施

- 12.1X46-D77
- 12.3X48-D70
- 12.3X54-D34
- 12.3R12-S10
- 12.3R13
- 14.1X53-D47
- 15.1X49-D140
- 15.1X53-D490
- 15.1X53-D471
- 15.1X53-D234
- 15.1X53-D67
- 15.1X53-D59
- 15.1R4-S9
- 15.1R7-S1
- 15.1R8
- 16.1R4-S9
- 16.1R6-S4
- 16.1R7
- 16.2R1-S7
- 16.2R2-S6

- 16.2R3
- 17.1R1-S7
- 17.1R2-S7
- 17.1R3
- 17.2R1-S6
- 17.2R2-S4
- 17.2R3
- 17.3R1-S5
- 17.3R2-S2
- 17.3R3
- 17.4R1-S4
- 17.4R2
- 18.1R2
- 18.2X75-D5
- 18.2R1

參考資料

1. <https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10898>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7183>
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