

**TLP:WHITE**

# 金融資安資訊分享與分析中心

## 弱點公告

(Cisco 發布 Network Convergence System 1000 系列設備漏洞)

發行日期：2019 年 02 月 22 日

# TLP:WHITE

## 摘要:

Cisco Network Convergence System 1000 系列設備使用的 IOS XR 軟體的 TFTP 服務存在漏洞，可允許未經身份驗證的遠端攻擊者於目標設備中檢視任意文件，因而可能導致資訊洩露。

## 概述:

該漏洞是由於該軟體未能正確驗證用戶於 TFTP 請求中的輸入資訊。攻擊者可於發送到目標設備上的 TFTP 服務的惡意請求中，使用目錄穿越技術來利用此漏洞。利用漏洞可允許攻擊者從目標設備檢索任意文件，從而導致洩露敏感資訊。

**影響軟/硬體廠牌:** Cisco Network Convergence System 1000 系列設備使用的 IOS XR 軟體。

## 影響版本/型號:

受影響軟體版本如下

Cisco IOS XR 6.5.2 之前版本，並須啟用 TFTP 服務。

## 影響程度:高

**CVE 編號:** CVE-2019-1681

## CVSS 向量:

## TLP:WHITE

使用版本：CVSS 3.0

分析分數：7.5(原廠自評)

分析向量：

攻擊向量 Network

攻擊複雜性 Low

需要專用權 None

使用者互動 None

範圍 Unchanged

機密性影響 High

完整性影響 None

可用性影響 None

資料來源：Cisco

防護方式：

請由參考連結之 URL 連至 Cisco 網站，根據廠商建議升級至無此漏洞之系統版本。

參考連結：

1. Cisco

**TLP:WHITE**

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-ncs>