Synology

Synology 安全性弱點回應政策

更新日期： 2024年5月6日

目錄

簡介

探索對您有幫助的資訊

- Synology 提供主題廣泛的技術支援文件。
- 您可以在知識中心找到有用的功能說明及常見問題文章，以及教學影片，將操作過程簡化為容易上手的小步驟。您也可以找到使用手冊、解決方案手冊、型錄、白皮書等文件。進階用戶及 IT 人員也可藉由管理手冊及開發手冊來找到需要的資源。
- 遇到問題或無法從官方文件找到解答時，也可嘗試在 Synology Community 尋求其他有經驗的使用者或技術支援團隊人員的協助。另外也可透過網頁表單、電子郵件、電話等方式聯絡 Synology 技術支援團隊。

作為 NAS 廠牌，Synology 推出不同系列產品，諸如私有雲裝置、網路通訊裝置、影像監控方案等。我們理解較舊型號裝置的安全性風險，以及補強安全問題的重要性。

本文將概述 Synology 的安全政策與具體措施，針對的產品包含 DiskStation Manager (DSM)、Synology Router Manager (SRM)、Synology 監控產品、BeeStation、Synology 開發的套件 (包含行動應用程式、桌面工具、Synology 發行的開源套件、協力廠商套件等)。Synology 提供多項服務讓各類用戶，從個人到企業，皆可自行架設私有雲。本文將說明 Synology 的安全性政策、Synology 如何辨識安全性威脅並歸類在適當的評級，以及 Synology 對安全性弱點的即時應變流程，例如每日回報通用漏洞披露 (Common Vulnerabilities and Exposures，CVE)。

Synology 保留不經預告而隨時修改本文的最終權利。若經修改，您可在 kb.synology.com 查閱最新版內容。請經常透過前述網址查閱本文，以便隨時獲悉最新資訊。

安全性政策

標準

Synology 致力於符合標準以提供安全性最佳實務運作。

Synolgoy 針對產品弱點並揭露給使用者及其他科技社群係的處理方式係依據下列工業標準及授權：

- ISO/IEC 29147：2018
- ISO/IEC 30111：2019
- FIRST 公共漏洞評分系統
- FIRST 交通燈協議
- FIRST PSIRT 服務框架
- Synology 目前參與以下安全性社群：
- CVE 編號管理者
- 事件回應及安全性團隊論壇 (FIRST)

嚴重性評級

Synology 主要基於公共漏洞評分系統 (CVSS) 來評估安全性問題的影響。依據各指標的基礎評分 (Base Score) 及時間性評分 (Temporal Score)，Synology 將以四分量表 (Critical、Important、Moderate、Low) 為安全性問題給予評級。

嚴重性是以安全弱點的技術分析決定，包含弱點類型、對應的潛在風險評估等。我們大致上依據公共漏洞評分系統 (CVSS) 3.1 版：FIRST 提供的規格文件。

這套嚴重性評級機制可幫助使用者了解 Synology 產品遭遇安全性弱點時的衝擊程度，並依據推薦的系統維護政策來修正弱點。因此，所有使用者將能透過下載對應的修復更新來保持系統穩定及安全性。

公共漏洞評分系統

公共漏洞評分系統 (CVSS) 是定義安全漏洞嚴重性的方式。

Synology 以 CVSS 3.1 版來評估弱點，此標準包含攻擊向量 (AV)、攻擊複雜度 (AC)、權限需求 (PR)、使用者互動 (UI)、範疇 (S)、機密性 (C)、整合度 (I)、可用性 (A) 等基本指標。漏洞的衝擊是以 0.0 至 10.0 分的評分範疇來呈現。若要進一步了解基本指標，請參閱 CVSS 3.1 版：使用手冊。

Synology 將依據 CVSS 3.1 版及前述的嚴重性評級規則來安排優先順序來修正弱點。

嚴重性評級

嚴重 (Critical) 衝擊

此等級為高風險的系統漏洞，當前尚未修正，且亟需盡速修正。

此評級的漏洞可能會讓未經身分認證的遠端人士自動觸發攻擊，並對至少兩個漏洞的面向帶來極大的衝擊：機密性 (C)、整合度 (I)、可用性 (A)

若有可行的補救措施 (RL：T)，嚴重性則可調降為 Important。

重要 (Important) 衝擊

此等級的漏洞對於尚未修正的系統不會帶來嚴重且立即的衝擊。

若攻擊行動受到身分驗證 (PR：L)、使用者互動 (UI：R)、非系統預設行為 (AC：H) 等牽制，將歸類為 Important 衝擊。

若有可行的補救措施 ，嚴重性則可調降為 Moderate。

但仍建議使用者在下個系統維護週期結束前修正漏洞或實施補救措施。

若服務有提供經身分認證的遠端使用者，管理員應針對受衝擊的系統盡速修正或實施補救措施。

此評級的漏洞可能會讓攻擊者觸發攻擊，並對至少一個漏洞的面向帶來極大的衝擊：機密性、整合度、可用性

中等 (Moderate) 衝擊

此評級的漏洞並不容易觸發攻擊 (AC：H)，但仍可能造成一定程度的衝擊，或可能在需要較高權限的情況下造成較大衝擊 (PR：H)。

輕微 (Low) 衝擊

此評級為其他安全性衝擊問題。此類漏洞通常很難觸發，或只能由管理員身分觸發。即便觸發也不會帶來重大衝擊。

Synology 安全性諮詢可能會包含多項弱點的修正更新，以及各種 Synology 產品的套件。每項安全性諮詢會針對不同產品進行評級。若有多個合併的問題，其整體嚴重性是以個別問題中最高嚴重性，或以最壞情境為準。

跨產品的基本評分差異

一個漏洞有不同 CVSS 基本指標的情況並不罕見，像是不同產品、型號、版本可能有不同影響範疇及嚴重性。Synology 會盡可能提供足夠的資訊，包含對應的嚴重性、CVSS 基本評分、攻擊向量等。若有安全性漏洞無法個別分開提列，我們將提列最壞的情況。

以下為一些範例：

- 僅影響特定產品的弱點。例如：CVE-2017-9417 僅影響 RT1900ac。
- 經來源碼保護機制或特定平台 Linux 安全模組進行補救的弱點。例如：CVE-2015-6912 可能在 DSM 5.0 上執行遠端程式碼，但在 DSM 5.1 上僅為阻斷服務 (DoS) 攻擊。

- 影響超過一款應用程式的弱點。例如：CVE-2017-9993 同時影響 DSM 及 Video Station，但對 Video Station 的 CVSS 評分及嚴重性較低。

NVD 及 Synology 評分差異

美國國家漏洞資料庫 (National Vulnerability Database，NVD) 或其他第三方漏洞資料庫針對單一 CVE 編號僅指定一種 CVSS 基本評分。但不同情境及設定選項可能存在差異極大的衝擊而有相當不同的評分。

例如：NVD 將 CVE-2017-1000367 評為 Medium 衝擊指標，理由是 sudo 被用以將有限的超級使用者權限提供給特定使用者。Synology 則針對 DSM 使用 Low 衝擊指標，因為 sudo 及 console 僅管理員有存取權限。

因此，相較於第三方評分方式，我們強烈建議客戶使用 Synology 安全性諮詢中的 CVSS 評分，並依循基於衝擊嚴重性的補救措施。若您對我們的安全性諮詢有任何建議或疑問，請隨時與我們聯絡，我們將視情況進行調整。

安全計畫

產品安全事件回應團隊 (PSIRT)

Synology PSIRT 負責管理與我們產品相關的安全性弱點資訊，包含接收、調查、合作、公開報告等措施。同時也是安全研究人員及其他機構的聯絡窗口，接受 Synology 潛在安全性弱點通報。

事件回應流程

Synology 處理安全性弱點並通知客戶的行動分為四個階段。

發現

我們對安全性弱點啟動調查並接收資訊的方式列舉如下：

- security@synology.com
- 電腦網路危機處理暨協調中心 (CERT/CC) 漏洞公告
- 國家級電腦網路危機處理中心 (例如：美國、台灣、日本等)
- 公開貼文 (Full Disclosure、oss-security、CVEnew 等)
- Synology 技術支援

我們鼓勵研究人員透過優良保密協定 (Pretty Good Privacy，PGP) 寄送概念驗證等敏感性訊息。當 PSIRT 從收到研究人員寄送的安全性通報後，將立即回覆以確認接收，並進行初步分析。在進入下一階段前，若缺乏釐清弱點的足夠資料時，可能會請求研究人員提供更多資訊。

鑑別

收到通報後，PSIRT 將開設臨時性的事件應變小組，成員包含：

- 相關監察員
- 研發部門及測試部門工程師
- 公關團隊

如果安全性弱點對我們產品造成衝擊，在 PSIRT 確認問題嚴重性及衝擊後，事件應變小組將檢核該通報並將相關問題記錄於 Synology 內部的追蹤系統。PSIRT 監察員負責安排時程並統籌資源來確保軟體修正更新發布流程順暢。

修復

PSIRT 將協助工程團隊來修復弱點或提出補救措施，並確保測試標準不會遷就於修復措施，例如確保不會造成功能毀損。PSIRT 會盡可能將修正更新交付研究人員來檢驗是否已妥善修復弱點。在此同時也會製作安全性諮詢。

揭露

完成安全性修復後，PSIRT 將發布安全性諮詢、更新 RSS 摘要，並寄送電子報說明該次安全性修復。同時，公關部門將宣傳並鼓勵軟體更新、收集客戶意見，並回報給 PSIRT。

若安全性弱點並非肇因於第三方軟體，PSIRT 將與 MITRE 共同為該弱點指派 CVE 編號。Synology 僅依揭露時程來發布安全性修復的詳情，並確保客戶在我們對外公布該弱點之前有足夠時間來安裝修正更新。研發人員可能會在公開訊息後揭露該弱點的詳情。

第三方軟體弱點

部分 Synology 產品有使用第三方或開源元件。當這些元件有安全性弱點被發現時，我們將參考 NVD 提供的報告或 CVSS 技術分析。Synology 將檢驗並鑑定該弱點對我們產品造成的衝擊，並進行評估。

若第三方的弱點影響到 Synology 產品，只要有下列任一情況，將視之為高度關注弱點：

- 該弱點吸引公眾的高度關注。
- 嚴重性評級為 Critical 或 Important。
- 該弱點可能被公開觸發，或被外界嘗試利用。

針對高度關注弱點，Synology 將啟動事件應變流程，評估所有維護中產品的潛在衝擊，並於第三方單位揭露相關資訊後發布安全性諮詢。其餘弱點將在發布修正更新後一併列於相關的發布資訊。

安全性發布類型

Synology 會在官方網站發布安全性諮詢及發行資訊附件。前述兩種文件的目的並不相同，分別針對不同的安全性問題。Synology 對所有公開文件上揭露的安全性弱點衝擊將保留最少資訊。我們不提供攻擊者如何利用弱點的詳情。

Synology 安全性諮詢

Synology 提供安全性諮詢來記錄影響我們產品的安全性問題。每項諮詢將以「Synology-SA-YY:NN」為標題，並依據 Critical、Important、Moderate、Low 等嚴重程度，或受公眾關注程度進行評級。所有諮詢皆以下列狀態來追蹤：

- Resolved (已解決)：已為受影響的所有產品修復該弱點。
- Ongoing (處理中)：Synology 已完成調查，並開發修正方式。
- Will not fix (不予修復)：Synology 評估決定不修復該弱點。
- Accepted (已受理)：Synology 已提升產品安全以防止嚴重漏洞。若裝置部屬弱點可控，且無嚴重安全性風險，將傾向不為裝置進行修復。

發行資訊附件

若已修復低嚴重性弱點，該弱點將以 CVE 編號或 Synology-SA 編號揭露於發行資訊。

	網站	電子郵件	RSS	社群媒體

安全性諮詢	Critical / Important 衝擊	有	選擇性	有	選擇性
	Moderate / Low 衝擊	有	選擇性	有	無
發行資訊附件		有	選擇性	無	無

CVE 編號管理者

CVE 編號管理者 (CVE Numbering Authority，CNA) 為全球各地獲授權指派 CVE 的機構，針對其自身清楚商定的產品範圍來首次公開新的安全性弱點。前述 CVE 會提供給研發人員、弱點揭露者、資訊科技業者等。

Synology 於 2017 年獲 MITRE 授權為 CNA 成員。成為 CNA 成員的主要差別是 Synology 獲授權可直接對 Synology 產品預配 CVE 編號。意即我們可與第三方研究人員合作，並在弱點資訊被公開之前先發布修正更新。研究人員通常需要 CVE 編號來進行確認，也較能依循我們的揭露政策。此流程可兼顧客戶的安全與彈性。

責任性揭露政策

Synology 遵照 90 天責任揭露政策時間軸。Synology 會在首次報告及衝擊評估的 90 天內發布軟體更新及安全性諮詢。

Synology 向使用者提供安全性諮詢來說明嚴重性及弱點影響範圍。但我們會保留概念驗證及觸發的詳情。例如攻擊向量、特定影響元件等細節將不會在 90 天內揭露。高嚴重性弱點可能會有額外寬限期，以確保多數使用者有足夠時間來計劃並部署軟體更新或補救措施。

在特殊情況下，Synology 仍保留偏離本政策的權利。

溝通計畫

於下列情況，Synology 可能會發布安全性諮詢：

- 修復弱點後，我們將發布安全性諮詢來通知使用者更新軟體。修復更新的版本將列於諮詢內容，若有補救措施也將一併公布。
- 高嚴重性弱點將提前發布安全性諮詢。
- 當弱點觸發事件蔓延時，Synology 將發布對應的安全性諮詢以告知使用者我們正在處理問題。若有補救措施也會同時公開。
- 針對第三方弱點，若影響範圍擴大或公眾關注提升時，Synology 會發布安全性諮詢或新聞稿。
- Synology 保留偏離本政策的權利以確保可於 www.synology.com 網站提供軟體修正更新。

事件回應資格

針對 Synology 產品涉及已知或疑似安全性弱點的事件，客戶將接收事件應變協助。

關於為使用者提供協助來解決事件，Synology 保留決定要如何執行以及隨時退出的權利。有關涉及人身、財產、網際網路，或執法單位及事件應變部門等造成實際或潛在威脅的安全性事件，Synology 會給予特別考量。

漏洞回報獎勵計畫 (Bounty Program)

Synology 非常重視客戶安全及產品的長期安全。Synology 配置資源以致力於在弱點被內部測試、研究人員，甚至客戶發現時能盡速修復。我們鼓勵安全性研究人員及所有使用者在發現任何安全性問題時，直接聯繫 Synology PSIRT 團隊。

PSIRT 將處理、辨識、判斷所有透過此表單收到的安全問題回報。PSIRT 承諾在收到回報的 7 個工作天內回覆。如需取得足夠資訊，則 PSIRT 盡可能在 30 個工作天內回覆。更多詳情請參閱安全問題回報獎勵計畫。

總結

Synology 致力於提供客戶穩定、安全的產品來儲存資料。資安與開發部門之間的積極合作，讓 Synology 得以迅速、有效率地修復安全性弱點。Synology 領先業界，為資料保護提供專業、強大的解決方案，讓各機構及個人用戶得以更專注於自身成長，降低網管維護成本。