Synology

Synology 安全性弱点应对政策

更新时间： May 6, 2024

目录

简介

查找您所需的信息

- Synology 发布了多种支持文档。
- 在知识中心中，您可以找到有用的帮助和常见问题文章，以及将过程划分成便捷步骤的视频教程。您还可以找到用户指南、解决方案指南、手册和白皮书。经验丰富的用户和管理员可在技术性管理员指南和开发人员指南中找到答案和指导。
- 您是否遇到了问题，并且无法在我们的官方文档中找到解决方案？可通过 Web 表单、电子邮件或电话联系 Synology 支持。

作为 NAS 供应商，Synology 提供各种设备，如私有云设备、路由器设备和监控解决方案。Synology 了解过时设备的安全性风险以及安全性修复的重要性。

本白皮书概述 Synology 的安全性和政策合规性方面的做法，针对的产品包括 DiskStation Manager (DSM)、Synology Router Manager (SRM)、Synology 监控产品、BeeStation、Synology 开发的套件（包括移动应用程序和桌面实用程序、Synology 发行的开放源代码套件以及合作伙伴套件）。Synology 提供多种服务让各类用户（从个人到企业）都可自行架设私有云。本白皮书说明了 Synology 的安全性政策、Synology 如何通过正确评级识别安全性威胁以及 Synology 针对漏洞的事件响应流程（例如每天报告通用漏洞与披露 (CVE)）。

Synology 保留随时更改本文档中任何内容的最终权利，恕不另行通知。如有任何更改，修订后的文档将在 kb.synology.cn 上提供。请查看此处所示的最新信息，以了解所有更改。

安全策略

标准

Synology 始终遵守标准，以便提供最佳安全做法。

Synology 遵循以下行业标准和要求对产品漏洞进行处理。这些标准和要求还有助于向我们的客户和更广泛的技术社区披露漏洞：

- ISO/IEC 29147:2018
- ISO/IEC 30111:2019
- FIRST 通用漏洞评分系统
- FIRST 交通灯协议
- FIRST PSIRT 服务框架
- Synology 目前加入了以下安全社区：
- CVE 编号机构
- 事件响应和安全团队论坛 (FIRST)

严重性评级

Synology 主要基于通用漏洞评分系统 (CVSS) 来评估安全性问题的影响。在收到按指标分配的基本分数和时间性分数后，Synology 将使用四分制（严重、重要、中等、轻微）对影响进行评级。

严重性通过对漏洞的技术分析（包括漏洞类型）以及对应的潜在风险评估来确定。我们通常参阅 FIRST 提供的通用漏洞评分系统 v3.1：规范文档。

此严重性评级机制可帮助用户了解安全性漏洞对 Synology 产品的影响，并根据建议的系统维护策略进行修复。因而用户随后都能够通过下载对应的修复来维护系统的稳定性和安全性。

通用漏洞评分系统

通用漏洞评分系统 (CVSS) 是一种定义漏洞严重性的方法。

Synology 使用 CVSS v3.1 标准评估漏洞，该标准包含攻击媒介 (AV)、攻击复杂性 (AC)、所需权限 (PR)、用户交互 (UI)、范围 (S)、机密性 (C)、完整性 (I) 和可用性 (A) 等基本指标。漏洞的影响以 0.0 到 10.0 分的评分范围来表示。若要了解有关基本指标的更多信息，请参阅通用漏洞评分系统 v3.1：用户指南。

Synology 将根据 CVSS v3.1 和上述严重性评级规则来决定修复漏洞的优先级。

严重性评级

严重影响

对于尚未修补的系统而言，这种级别的漏洞存在很高风险，必须尽快修补。

此评级针对未通过验证的远程攻击者可以自动利用的缺陷，对漏洞的至少两个方面具有持续重大影响：机密性 (C)、完整性 (I) 和可用性 (A)。

如果有缓解措施可用 (RL:T)，则严重性可调整为重要。

重要影响

这种级别的漏洞不会对未修补系统产生严重和直接影响。

如果攻击需要验证 (PR:L)/用户交互 (UI:R) 或非系统默认行为 (AC:H)，则会将其归类为重要影响。

如果有缓解措施可用，则严重性可调整为中等。

但是，仍建议用户在下一个系统维护周期结束前修补漏洞或应用缓解措施。

如果向经过身份验证的远程用户提供服务，则管理员应尽快修补受影响的系统或应用缓解措施。

此评级针对攻击者可以利用的缺陷，对漏洞的至少一个方面具有持续重大影响：机密性、完整性和可用性。

中等影响

此评级分配给难以利用 (AC:H) 但仍可能会造成一定程度的影响的缺陷，或者分配给可能会导致重大影响但需要高权限 (PR:H) 的缺陷。

轻微影响

此评级分配给所有其他具有安全性影响的问题。通常难以触发对这些类型的漏洞的利用，或只能由管理员触发。即使触发，影响也极低。

Synology 安全顾问可能包含针对多个漏洞的修补程序以及各种 Synology 产品的套件。每个安全顾问都包含针对每个产品的评级。总体严重性来自所有单个问题中的最高严重性，或组合所有问题时的最坏情况。

各产品间的基本分数差异

漏洞通常具有不同的 CVSS 基本指标，即不同的范围和严重性，具体取决于产品、型号或版本。Synology 将提供尽可能多的信息，包括对应的严重性、CVSS 基本分数和媒介。如果我们无法区分每个漏洞，则会报告最坏的结果。

这种情况的示例包括：

- 仅影响特定产品的漏洞。例如，CVE-2017-9417 仅影响 RT1900ac。
- 在某些平台上可通过源代码保护机制或 Linux 安全模块进行缓解的漏洞。例如，CVE-2015-6912 可能会在 DSM 5.0 上导致任意代码执行，但在 DSM 5.1 上只是拒绝服务攻击。
- 影响多个应用程序的漏洞。例如，CVE-2017-9993 同时影响 DSM 和 Video Station，但对于 Video Station 具有较低的 CVSS 分数和严重性。

NVD 与 Synology 分数之间的差异

美国国家漏洞数据库 (NVD) 或其他第三方漏洞数据库只会向单个 CVE ID 分配一个 CVSS 基本分数。但是，不同方案和配置选项可能会产生显著不同的影响，分数可能会相差很大。

例如，NVD 将 CVE-2017-1000367 评级为具有中等影响指标，因为 sudo 用于向特定用户提供有限的超级用户权限。对于 DSM，我们使用低等影响指标，因为 sudo 和控制台只能由管理员访问。

因此，强烈建议客户使用 Synology 安全顾问中的 CVSS 分数，并根据严重性影响采取缓解策略，而不是使用来自第三方的评估分数。如果您对我们的安全顾问有任何建议或疑问，请联系我们，我们将在必要时调整安全顾问。

安全性计划

产品安全性事件响应团队

Synology PSIRT 负责管理与 Synology 产品相关的安全性漏洞信息的收集、调查、协调和公开报告事宜。也是安全性研究人员和其他组织报告 Synology 潜在安全性漏洞的联系方。

事件响应流程

Synology 分四个阶段处理漏洞并通知我们的客户。

发现

我们主动调查漏洞并通过以下方式（包括但不限于）接收信息：

- security@synology.com
- CERT/CC 漏洞公告
- 国家 CERT（US-CERT、TWCERT/CC、JPCERT/CC 等）
- 公开发布（全面披露、oss-security、CVEnew 等）
- Synology 支持

我们鼓励研究人员通过优良保密协议（Pretty Good Privacy，PGP）加密发送敏感消息（如概念证明）。一旦 PSIRT 收到研究人员的安全性报告，他们将立即进行响应以确认接收，并进行简单分析。如果在进入下一阶段之前缺少足够的信息来阐释漏洞，研究人员可能会需要提供更多信息。

鉴别

收到报告后，PSIRT 将临时组建一个由以下人员组成的事件响应团队：

- 相关监督者
- 研发团队和质量控制团队的工程师
- 公共关系团队

如果漏洞会对我们的产品产生影响，则事件响应团队将对报告进行核验，并在 PSIRT 确认问题的严重性和影响之后将对应的错误记录在跟踪系统中。PSIRT 监督者会负责安排计划和协调资源，以确保软件补丁发布过程顺利进行。

修正

PSIRT 将协助工程团队修复漏洞或找到缓解措施，并确保测试质量不会因修复而受到影响，例如导致功能损毁。如果可能，PSIRT 会将补丁提交给研究人员进行验证，以确保正确修复漏洞。同时会生成安全顾问。

披露

应用安全性修复后，PSIRT 将发布安全顾问、更新 RSS 源并发送有关安全性修复的通讯电子邮件。同时，公共关系团队会推广软件更新、收集用户反馈并向 PSIRT 报告。

如果漏洞不是由第三方软件所导致，PSIRT 将与 MITRE 合作并为漏洞分配 CVE ID。Synology 只会在缺陷发布一段合适时间之后根据披露计划发布安全性修复的详细信息，以确保我们的客户有足够的时间安装补丁。研究人员可能会在公开披露之后披露漏洞的详细信息。

第三方软件漏洞

某些 Synology 产品基于第三方或开放源代码组件而构建。当在这些组件中发现漏洞时，我们将参阅 NVD 提供的报告或 CVSS 技术分析。Synology 将验证并鉴别缺陷对我们产品的影响，并进行评估。

如果第三方漏洞会影响 Synology 产品，则在满足以下条件之一时将漏洞视为“高风险”：

- 漏洞引起了公众的极大关注。
- 严重性评级评估为关键或重要影响。
- 漏洞可能会被公开利用，或概念证明已公开。

对于高风险漏洞，Synology 将开始事件响应流程，评估所有仍在进行维护的潜在受影响产品，并在第三方披露相关信息后发布安全顾问。所有其他漏洞都将在修补之后在相关发行说明中列出。

安全性发布文件的类型

Synology 会在官方网站上发布安全顾问和发行说明附件。这两份文档具有不同用途，涵盖不同的安全性缺陷。Synology 披露的漏洞影响相关信息是所有发布文件中最少的。不会提供攻击者可能会利用的漏洞详细信息。

Synology 安全顾问

Synology 提供安全顾问，记录影响 Synology 产品的安全性缺陷。每个安全顾问以 Synology-SA-YY:NN 命名，并根据严重、重要、中等或轻微严重性评级对漏洞进行评级，或是评级为受公众关注的漏洞。所有安全顾问都使用以下状态进行跟踪：

- 已解决：已为所有受影响的产品修复指定漏洞。
- 正在进行：Synology 已完成调查，正在制定修复措施。
- 不会修复：Synology 决定不修复产品的漏洞。
- 已接受：Synology 已增强其产品来防止严重漏洞。如果设备部署漏洞可控且没有严重安全性风险，则设备不会进行修复。

发行说明附件

如果修复了轻微严重性漏洞，将按 CVE ID 或 Synology-SA ID 在发行说明中披露这些漏洞。

	网站	电子邮件	RSS	社交媒体

安全顾问	严重/重要影响	是	可选	是	可选
	中等/轻微影响	是	可选	是	否
发行说明附件		是	可选	否	否

CVE 编号机构

CVE 编号机构 (CNA) 是来自世界各地的组织，这些组织经过授权可在其同意的明确范围内将 CVE 分配给影响产品的漏洞，以便在新漏洞的首次公开公告中包含这些信息。这些 CVE 将提供给研究人员、漏洞披露者和信息技术供应商。

MITRE 于 2017 年将 Synology 授权为 CNA 成员。CNA 成员与非 CNA 制造商之间的主要区别在于，Synology 已经过认证，可直接将 CVE ID 预分配给 Synology 产品。这意味着我们可以与第三方研究人员合作，可在不先发布任何漏洞信息的情况下发布修复。研究人员通常需要 CVE ID 进行确认，并愿意遵守我们的披露政策。通过此流程，我们的客户可以同时获得安全性和灵活性。

负责任的披露政策

Synology 遵循 90 天负责任的披露政策时间线。Synology 会在首次报告和影响评估后的 90 天内发布软件更新和安全顾问。

Synology 为用户提供安全顾问，以说明漏洞的严重性和范围。但是，Synology 会保留任何概念证明和利用细节。详细信息（如攻击媒介和特定受影响组件）将不会在 90 天内披露。对于高严重性漏洞，可能会使用更长的额外宽限期，以确保足够的用户有足够的时间来规划和部署更新或缓解措施。

Synology 保留在极端情况下偏离本政策的权利。

通信计划

在以下情况下，Synology 可能会考虑发布安全顾问：

- 在 Synology 修复漏洞后，我们将发布安全顾问以通知用户更新其软件。补丁版本将在安全顾问中列出，并且包含缓解措施（如果可用）。
- 将提前发布安全顾问，以解决高严重性漏洞。
- 当攻击开始传播时，Synology 会发布对应的安全顾问，以通知用户我们正在解决问题。如有可用缓解措施，也会进行发布。
- 对于第三方漏洞，如果范围扩大或公众关注度增加，Synology 会发布安全顾问或发布公开公告。
- Synology 保留偏离本政策的权利，以确保在 www.synology.cn 上提供软件补丁。

事件响应资格

对于涉及 Synology 产品中的已知或合理怀疑安全性漏洞的事件，客户会获得事件响应帮助。

Synology 保留决定向用户提供何种帮助来解决事件或随时退出任何事件的权利。对于涉及人身、财产、网络的实际或潜在威胁的安全性事件，或者来自执法机构和官方事件响应团队的请求，Synology 可能会给予特殊考虑。

赏金计划

Synology 致力于确保客户安全和产品的长期安全性。在内部测试、研究人员或客户发现漏洞后，Synology 会立即分配资源来修复漏洞。Synology 鼓励安全性研究人员和所有用户在发现任何安全性相关问题时直接联系 Synology PSIRT。

PSIRT 会处理、识别和判断通过安全表单收到的所有安全性报告。PSIRT 保证在收到报告后的 7 个工作日内进行回复。在获得安全性报告的所需信息后，PSIRT 会努力在 30 个工作日内进行回复。如需了解更多信息，请参阅安全性错误赏金计划。

结论

为我们的客户提供可靠、安全的产品来存储其数据始终是 Synology 的首要使命。我们安全性计划团队与产品开发团队之间的积极协作使 Synology 能够快速高效地修复安全性漏洞。借助我们强大且专业的数据保护解决方案（只有少数 NAS 公司能提供），组织和个人现在可以更加专注于其业务并降低 IT 成本。