Synology

# Synology Vulnerability Response Policy

Last May 6, 2024

# Table of Contents

# Introduction

**Find your information**

- Synology publishes a wide range of supporting documentation.
- In Knowledge Center, you will find useful Help and FAQ articles, as well as video tutorials breaking up processes into handy steps. You can also find User's Guides, Solution Guides, brochures, and White Papers. Experienced users and administrators will find answers and guidance in technical Administrator's Guides and Developer Guides.
- Got a problem and unable to find the solution in our official documentation? Search hundreds of answers by users and support staff in Synology Community or reach Synology Support through the web form, email or telephone.

As a NAS vendor, Synology provides a variety of devices, such as private cloud devices, router devices, and surveillance solutions. Synology understands the security risks on out-of-date devices and the importance of security fixes.

This white paper outlines Synology's approach to security and policy compliance for DiskStation Manager (DSM), Synology Router Manager (SRM), Synology Surveillance products, BeeStation, Synology-developed packages including mobile applications and desktop utilities, Synology-distributed open source packages, and partner packages. From personal to enterprise, Synology offers various services for you to make your own private cloud up and running. This paper illustrates Synology's security policy, how Synology identifies security threats with proper ratings, and Synology's incident response flow against vulnerabilities, such as reporting Common Vulnerabilities and Exposures (CVE) day-by-day.

Synology reserves the final right to change any content in this document at any time without prior notice. In the event of any changes, the revised document will be available on kb.synology.com. Please check the latest information indicated herein to inform yourself of any changes.

# Security Policy

## Standards

Synology is committed to adhering to standards in order to provide the best practices for security.

The following industry standards and mandates guide the handling of product vulnerabilities at Synology. They also facilitate the disclosure of vulnerabilities to our customers and the broader technology community:

- ISO/IEC 29147:2018
- ISO/IEC 30111:2019
- FIRST Common Vulnerability Scoring System
- FIRST Traffic Light Protocol
- FIRST PSIRT Services Framework
- Synology is currently participating in the following security communities:
- CVE Numbering Authorities
- Forum of Incident Response and Security Teams (FIRST)

## Severity Ratings

Synology primarily evaluates the impact of security issues based on the Common Vulnerability Scoring System (CVSS). After receiving the Base Score and Temporal Score assigned by the metrics, Synology will use a four-point scale (Critical, Important, Moderate, Low) to rate the impact.

The severity is determined through a technical analysis of the vulnerability, including the type of vulnerability, and the corresponding potential risk assessment. We generally refer to the Common Vulnerability Scoring System v3.1: Specification Document provided by FIRST.

This severity rating mechanism helps users understand the impact of security vulnerabilities on Synology products, and fix them according to the recommended system maintenance policies. All users will then be able to maintain system stability and security by downloading the corresponding fixes.

### Common Vulnerability Scoring System

Common Vulnerability Scoring System (CVSS) is a method for defining the severity of a vulnerability.

Synology assesses vulnerabilities using the CVSS v3.1 standards, which include the base metrics Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR), User Interaction (UI), Scope (S), Confidentiality (C), Integrity (I), and Availability (A). The impact of a vulnerability is represented by a score ranging from 0.0 to 10.0. To learn more about base metrics, please refer to Common Vulnerability Scoring System v3.1: User Guide.

Synology will decide the priority with which vulnerabilities should be fixed based on CVSS v3.1 and the rules of severity rating mentioned above.

## Severity Rating

### Critical Impact

This level of vulnerability is high risk for systems that have not been patched, and must be patched as soon as possible.

This rating is given to flaws that can be automatically exploited by unauthenticated remote attackers, and have a great impact on at least two constant aspects of a vulnerability: Confidentiality (C), Integrity (I), and Availability (A).

If mitigation is available (RL:T), the severity may be adjusted as Important.

### Important Impact

This level of vulnerability does not have a serious and immediate impact on unpatched systems.

If the attacks require authentication (PR:L), user interaction (UI:R), or non-system default behavior (AC:H), it will be classified as Important impact.

If mitigation is available, the severity may be adjusted as Moderate.

However, users are still suggested to patch the vulnerabilities or apply mitigations before the end of the next system maintenance cycle.

If services are provided to authenticated remote users, administrators should patch or apply mitigations to impacted systems as soon as possible.

This rating is given to flaws that can be exploited by attackers and have a great impact on at least one constant aspect of a vulnerability: Confidentiality, Integrity, and Availability.

### Moderate Impact

This rating is assigned to flaws that are difficult to exploit (AC:H) but could still cause a certain level of impact, or is assigned to flaws that could lead to significant impact but requires high privilege (PR:H).

### Low Impact

All other issues that have a security impact are assigned this rating. The exploits of these types of vulnerability are usually difficult to be triggered, or could only be triggered by an administrator.

Even if they are triggered, the impact is minimal.

A Synology security advisory may contain patches for multiple vulnerabilities as well as packages for various Synology products. Every security advisory has a rating for each product. The overall severity is taken from the highest severity out of all the individual issues or the worst-case scenario when all the issues are combined.

### Base Score Variations Across Products

It is common for a vulnerability to have different CVSS base metrics, i.e. different scope and severity, depending on the product, model, or version. Synology will provide as much information as possible, including the corresponding severity, CVSS base score, and vector. If we are unable to separate each vulnerability, we will report the worst outcome.

Examples of this include:

- A vulnerability that only affects certain products. For example, CVE-2017-9417 only affects RT1900ac.
- A vulnerability that is mitigated by source code protection mechanisms or Linux Security Modules on some platforms. For example, CVE-2015-6912 could have led to arbitrary code execution on DSM 5.0, but it is only a denial-of-service attack on DSM 5.1.
- A vulnerability that affects more than one application. For example, CVE-2017-9993 affects both DSM and Video Station, but has a lower CVSS score and severity for Video Station.

### Differences Between NVD and Synology Scores

National Vulnerability Database (NVD) or other third-party vulnerability databases will only assign one CVSS base score to a single CVE ID. However, different scenarios and configuration options may have significantly different impacts and the scores can vary widely.

For example, NVD rates CVE-2017-1000367 to have Medium impact metrics because sudo is used to provide limited super user privileges to specific users. For DSM, we use Low impact metrics, as sudo and the console are only accessible by the administrator.

As a result, instead of using evaluated scores from third parties, we strongly suggest our customers use the CVSS score in the Synology Security Advisory and follow the mitigation strategy based on the severity impact. If you have any suggestions for or concerns about our Security Advisory, please contact us and we will adjust the Security Advisory if necessary.

# Security Program

## Product Security Incident Response Team

Synology PSIRT manages the receipt, investigation, coordination, and public reporting of security vulnerability information related to Synology products. It is also the contact for security researchers and other organizations to report potential Synology security vulnerabilities.

### Incident Response Process

There are four stages with which Synology handles vulnerabilities and notifies our customers.

#### Discovery

We take the initiative to investigate vulnerabilities and to receive information including but not limited to the following ways:

- security@synology.com
- CERT/CC Vulnerability Notes
- National CERTs (US-CERT, TWCERT/CC, JPCERT/CC, etc.)
- Public posting (Full Disclosure, oss-security, CVEnew, etc.)
- Synology Support

We encourage researchers to send sensitive messages such as proof-of-concept through Pretty Good Privacy (PGP) encryption. Once PSIRT receives security reports from researchers, they will respond immediately to confirm receipt, and make a simple analysis. Researchers may be asked to provide further information if there is insufficient information to clarify the vulnerabilities before going to the next stage.

#### Triage

After receiving the report, PSIRT will build a temporary incident response team consisting of:

- Relevant supervisors
- Engineers of R&D team and Quality Control team
- Public Relation team

If the vulnerability comes with an impact on our products, the incident response team will verify the report and will log the corresponding bug into our tracking system after the PSIRT confirms the severity and impact of the issue. The PSIRT supervisor is responsible for arranging the schedule and coordinating resources to ensure that the software patch release process is executed smoothly.

### Remediation

PSIRT will assist the engineering team in fixing the vulnerability or finding a mitigation, and will ensure that the quality of the test will not be compromised due to the fix, such as causing a functional crash. If possible, PSIRT will submit the patch to researchers for verification to make sure that the vulnerabilities are fixed properly. A security advisory will be produced at the same time.

### Disclosure

After applying the security fix, PSIRT will publish a security advisory, update the RSS feed, and send an e-news email about the security fix. Meanwhile, the Public Relation team will promote the software update, collect user feedback and report back to PSIRT.

If the vulnerability is not caused by third-party software, PSIRT will work with the MITRE to assign a CVE ID to the vulnerability. Synology will only release the details of the security fix according to the Disclosure Schedule, and after the flaw has been published for a suitable period of time to ensure that our customers have enough time to install the patch. Researchers may disclose the details of the vulnerability after the public disclosure.

## Third-Party Software Vulnerabilities

Some Synology products are built on third-party or open source components. When a vulnerability is discovered in these components, we will refer to the report or CVSS technical analysis provided by NVD. Synology will verify and triage the impact of the flaws on our products, and give our evaluation.

If a third-party vulnerability affects Synology products, the weakness will be considered high-profile if one of the following conditions is met:

- The vulnerability has attracted significant public attention.
- The Severity Rating is evaluated as a Critical or Important impact.
- The vulnerability is likely to be exploited publicly or have a public proof-of-concept.

For high-profile vulnerabilities, Synology will begin the Incident Response process, evaluate all potentially impacted products that are still under maintenance, and publish a Security Advisory after a third party discloses related information. All other vulnerabilities will be listed in the relevant release notes after being patched.

## Types of Security Publications

Synology publishes Security Advisories and release note enclosures on the official website. These two documents have different intentions, and cover different security flaws. Synology keeps minimum information about the impact of the vulnerabilities disclosed on all publications. No vulnerability details that may be exploited by attackers will be provided.

### Synology Security Advisories

Synology provides Security Advisories that record security flaws affecting Synology products. Each advisory is entitled as Synology-SA-YY:NN, and will rate vulnerabilities according to the Critical, Important, Moderate, or Low severity rating or a vulnerability subject to public concern. All advisories are tracked using the following statuses:

- Resolved: The specified vulnerabilities are remediated for all affected products.
- Ongoing: Synology has completed the investigation, and is developing the remediation.
- Will not fix: Synology has decided not to remediate the vulnerability for the product.
- Accepted: Synology has enhanced its products to prevent serious vulnerabilities. If a device deployment vulnerability is controllable and is not under a critical security risk, the device is not subject to remediation.

### Release Note Enclosures

If low severity vulnerabilities are remediated, these vulnerabilities will be disclosed in the release notes by CVE IDs or Synology-SA IDs.

| | | Website | Email | RSS | Social Media |
|---|---|---|---|---|---|
| Security Advisories | Critical / Important Impact | Yes | Optional | Yes | Optional |
| | Moderate / Low Impact | Yes | Optional | Yes | No |
| Release Note Enclosures | | Yes | Optional | No | No |

# CVE Numbering Authority

CVE Numbering Authorities (CNAs) are organizations from around the world that are authorized to assign CVEs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities. These CVEs are provided to researchers, vulnerability disclosures, and information technology vendors.

Synology was authorized as a CNA member by MITRE in 2017. The major difference between a CNA member and a non-CNA manufacturer is that Synology is certified to directly pre-allocate CVE IDs to Synology products. This means that we can cooperate with third-party researchers, and release fixes without publishing any vulnerability information first. The researchers usually need CVE IDs for confirmation and are willing to follow our disclosure policy. Through this process, our customers can get security and flexibility at the same time.

## Responsible Disclosure Policy

Synology follows a 90-day responsible disclosure policy timeline. Synology issues software updates and security advisories within 90 days of the initial reports and impact assessment.

Synology provides users with security advisories to explain the severity and the scope of the vulnerability. However, Synology will withhold any proof-of-concept and exploit details. Details such as attack vectors and specific affected components will not be disclosed within 90 days. An additional grace period longer may be utilized for high-severity vulnerabilities to ensure enough users have adequate time to plan for and deploy updates or mitigation.

Synology reserves the right to deviate from this policy under extreme circumstances.

## Communications Plan

Under the following circumstances, Synology may consider publishing security advisories:

- After Synology fixes the vulnerabilities, we will publish security advisories to notify users to update their software. Patch versions will be listed in the advisories and mitigation will be included, if available.
- Security advisories will be published in advance to address high-severity vulnerabilities.
- When exploits start to spread, Synology publishes corresponding security advisories to notify users that we are addressing the issue. Mitigation will also be published, if available.
- For third-party vulnerabilities, Synology publishes security advisories or makes a public announcement if the scope expands or public awareness increases.
- Synology reserves the right to deviate from this policy to ensure software patch availability on www.synology.com.

## Incident Response Eligibility

Customers will receive incident response assistance for incidents involving known or reasonably suspected security vulnerabilities in a Synology product.

Synology reserves the right to decide what kind of assistance to offer users to solve the incident, or to withdraw from any incident at any time. Synology may give special consideration for security incidents that involve actual or potential threats to persons, property, the Internet, or requests from law enforcement agencies and formal incident response teams.

## Bounty Program

Synology is committed to customer safety and the long-term security of our products. Synology allocates resources to fix vulnerabilities as soon as they are discovered by internal tests, researchers, or customers. Synology encourages security researchers and all users to contact Synology PSIRT directly if they discover any security-related issues.

PSIRT processes, identifies, and judges all security reports received from the security form. PSIRT guarantees to respond within 7 working days after receiving the report. After obtaining necessary information for the security report, PSIRT endeavors to respond within 30 days working days. For more information, please refer to the Security Bug Bounty Program.

# Conclusion

Providing our customers with reliable and secure products on which to store their data has always been Synology's primary consideration. The active collaboration between our security program team and product development team enables Synology to fix security vulnerabilities quickly and efficiently. With our powerful and professional solutions for data protection that only few NAS companies have, organizations and individuals can now focus more on their businesses and reduce IT costs.