Synology Security Whitepaper

Synology®

Table of Contents

Introduction 3

Security Policy 4

- DiskStation Manager Life Cycle
- Severity Ratings
- Standards

Security Program 10

- Product Security Incident Response Team
- Bounty Program

Conclusion 15

Introduction

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 Synology understands the security risks on out-of-date devices and the importance of security fixes.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 whitepaper outlines Synology's approach to security and policy compliance for our major product, Synology DiskStation Manager (DSM). From personal to enterprise, DSM offers storage and services for you to set up your own private cloud. This paper illustrates Synology's security policy, how Synology identifies security threats with proper ratings, how Synology handles your private data, and Synology's incident response flow against security threats, such as reporting CVEs day-by-day.

Security Policy

DiskStation Manager Life Cycle

Synology offers software update services for each minor release of DSM throughout three life-cycle phases: Production 1, Production 2, and Extended Life Phase.

During three life-cycle phases, Synology may release qualified Critical and Important security fixes, as well as selected and high priority bug fixes. Also, we will issue their corresponding security advisories (Synology-SA-YY:NN) or bug fix notes. Other security fixes or bug fixes may be delivered as appropriate.

If available, selected enhanced software functionalities, and new or improved hardware enablements may be provided at the discretion of Synology.

The DSM life-cycle phases are designed to let users know when and what to update within each minor release over time.

Details

Each minor version of DSM, such as DSM 6.1, is identified as a different product with a different number of life-cycles. Some of them will have an extended life phase and are identified as Long Term Support. Security fixes, bug fixes, software enhancements, or hardware enablements may be contained in each phase.

Software changes to DSM will be delivered via individual updates as the smallest version changes, such as DSM 6.1.3-4, or be aggregated as a larger release, such as DSM 6.1.3. The following table lists the differences between each phase:

Description	Production 1	Production 2	Extended Life Phase
Security Errata	Yes	Yes	Yes
Bug Fix Errata	Yes	Yes	Yes
Software Enhancements	Yes	No	No
Hardware Enablements	Yes	No	No

LTS (Long Term Support)

Among DSM major versions, such as DSM 6.x, Synology marks at least one minor version as Long-Term-Support (LTS). LTS version has three life cycles: Production 1, Production 2, and Extended Life. While other versions have only two life-cycle phases: Production 1 and Production 2.

Production Phases

- Production 1 Phase

During Production 1 Phase, qualified Critical and Important security fixes, and urgent and selected high priority bug fixes may be released as they become available. Other fixes may be delivered as appropriate.

If available, selected enhanced software functionalities, and new or improved hardware enablements may be provided at the discretion of Synology.

- Production 2 Phase

During Production 2 Phase, only qualified Critical impact security fixes, selected and urgent priority bug fixes may be released as they become available. Other fixes may be delivered as appropriate.

New functionalities and new hardware enablements will not be released in Producstion 2 Phase.

- Extended Life Phase

During Extended Life Phase, only qualified Critical impact security fixes and selected urgent priority bug fixes may be released as they become available. Other fixes may be delivered as appropriate.

Extended Life Phase is not included in every DSM version. It is an additional software update service for LTS versions.

Life-cycle Dates

All future dates mentioned for "End of Production 1" and "End of Production 2" are close approximations, non definitive, and subject to change.

Version	General Availability	End of Production 1	End of Production 2	End of Extended Life Phase
4.2 (LTS)	2013/03	2014/06	2015/06	2017/06
4.3	2013/08	2014/12	2015/12	N/A
5.0	2014/03	2015/06	2016/06	N/A
5.1	2014/11	2015/12	2016/12	N/A
5.2 (LTS)	2015/05	2016/06	2017/06	2019/06
6.0	2016/03	2017/06	2018/06	N/A
6.1	2017/03	2018/06	2019/06	N/A
6.2	~Q1 of 2018	2019/06	2020/06	TBD

Severity Ratings

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

The severity is based on the 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 v3.0: 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. In this way, all users will be able to download the corresponding fixes to maintain system stability and security.

Severity Rating	Description
Critical impact	• This level of vulnerability is highly risky for systems that have not been fixed, and need to be fixed 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 the attacks require authentication (PR:L)/user interaction (UI:R)/non-system default behavior (AC:H), it will not be classified as Critical impact. • If mitigation is available (RL:T), the severity may be adjusted from Critical to Important.
Important impact	• This level of vulnerability does not have serious and immediate impact on unfixed systems. However, users are still suggested to fix the vulnerabilities or apply mitigations before the end of the next system maintenance cycle. • Users should fix or apply mitigations to influenced systems as soon as possible if services are provided to authenticated remote users. • 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. • If mitigation is available, the severity may be adjusted to Moderate.
Moderate impact	• This rating is given to flaws that are difficult to be exploited (AC:H) but could still cause a certain level of impact, or is given to flaws that could lead to significant impact but needs high authority (PR:H).
Low impact	• This rating is given to all the other flaws that have a security impact. 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 very limited.

A Synology security advisory may contain fixes for more than one vulnerability and packages for different products. Every security advisory has a rating for each product. The overall severity is the highest severity out of all the individual issues, or the worst circumstances of combining all the issues.

Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System (CVSS) provides a way to define and evaluate the severity of a vulnerability.

Synology adopts the standard of CVSS v3.0, and evaluates vulnerabilities by 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 from 0 to 10. To learn more about base metrics, please refer to **Common Vulnerability Scoring System v3.0: User Guide**.

Synology will decide the priority with which vulnerabilities should be fixed based on CVSS v3.0 and the rules of severity rating mentioned above.

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, and list the corresponding severity, CVSS base score and vector. If we are not able 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

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 as having Medium impact metrics because the *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 the evaluated scores of the third party, we strongly suggest our customers to use the CVSS score in the Synology Security Advisory, and to 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.

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 29147:2014(E) - **Information technology -- Security techniques -- Vulnerability disclosure**
- ISO/IEC 30111:2013(E) - **Information technology -- Security techniques -- Vulnerability handling processes**

Synology is currently participating in the following security community:

- **CVE Numbering Authorities**

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.

- Stage 1: Report

We take the initiative to investigate vulnerabilities and to receive information in the following ways:

- **security@synology.com**
- Public posting (Full Disclosure, oss-security, CVEnew, etc.)
- **Synology Support**

We encourage researchers to send sensitive messages such as proof of concept through PGP encryption. Once PSIRT receives security reports from researchers, they will respond immediately to confirm that we have received the reports, and make a simple analysis. If there is not enough information, researchers may be asked to provide more information to clarify the vulnerabilities before going to the next stage.

- Stage 2: Validate and Triage

After receiving the report, PSIRT will build a temporary emergency security team consisted by:

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

If the vulnerability will have an impact on our products, the emergency security team will verify the report, and log the corresponding bug in our bug system after the PSIRT confirms the severity and impact of the issue. Our supervisor will be responsible for arranging the schedule and coordinating resources to ensure that the software patch release process is executed smoothly.

- Stage 3: Remediate

PSIRT will assist the engineering team in fixing the vulnerability or finding a mitigation, and 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, and produce the security advisory at the same time.

- Stage 4: Disclose

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, Public Relations will promote the software update, collect user feedback and report back to PSIRT. If any incorrect security fixes or negative impact has been discovered, PSIRT will recall the software update and develop a more suitable security fix.

If the vulnerability is not caused by a third-party software, PSIRT will work with MITRE corporation and 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 attack after the release.

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 re-examine the impact of the flaws on our products, and give our evaluation.

If a third-party vulnerability affects our 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 public proof of concept.

For high profile vulnerabilities, Synology will start 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 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. However, Synology keeps minimum information about the impact of the vulnerabilities disclosed on all publications. Synology will not provide any vulnerability details that may be exploited by attackers.

- 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.

- Release Note Enclosures

Security issues with a Low Impact Rating will be disclosed in release notes by CVE IDs or Synology-SA IDs.

The following table summarizes the channels we use to notify customers about the security publications. Ways of communication may be adjusted based on different needs.

<table>
<tr><th colspan="2"></th><th>Website</th><th>Email</th><th>RSS</th><th>Social Media</th></tr>
<tr><td rowspan="2">Security Advisories</td><td>Critical and Important Impact</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Optional</td></tr>
<tr><td>Moderate and Low Impact</td><td>Yes</td><td>Yes</td><td>Yes</td><td>No</td></tr>
<tr><td colspan="2">Release Note Enclosures</td><td>Yes</td><td>No</td><td>No</td><td>No</td></tr>
</table>

- CVE Numbering Authority (CNA)

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 disclosers, 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. We will issue software updates and security advisories within 90 days from when we receive the reports and confirm the impact. To complete the CVE assigning process, the corresponding CVE ID and the details of the vulnerability will be released on the last day. There will be a 14-day grace period for high risk vulnerabilities.

To ensure that users have enough time to install the patch, Synology will provide users with the corresponding security advisories to explain the severity and the scope. However, we will not reveal any proof of concept. Vulneralbility details such as attack vector and certain affected components will not be disclosed within 90 days.

Synology reserves the right to deviate from this policy to ensure software patch availability on **Synology's official website**.

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 mitigations will be included, if available.
- Security advisories will be published in advance to address high-severity vulnerabilities.
- When attack programs starts to spread, Synology will publish corresponding security advisories to notify users that we are addressing the issue. Mitigations will also be released, if available.
- For third-party vulnerabilities, Synology will publish security advisories or make 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 Synology.com.

Incident Response Eligibility

Customers 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. We 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. We allocate resources to fix vulnerabilities as soon as they are discovered by internal tests, researchers, or customers. We encourage security researchers and all users of Synology to contact Synology PSIRT directly if they discover any security-related issues.

Since 2015, Synology has held several bounty program events. In 2015, Synology joined HITCON Hack2Own, and discovered several security issues in this event. In 2016, Synology held a private bounty event, and invited several security research groups. In 2017, Synology held a public bounty program, and received several security issue reports.

Synology PSIRT will process, identify, and judge all security reports received at **bounty@synology.com**. Synology guarantees to respond within two working days after receiving the report. After obtaining necessary information for the security report, we will endeavor to respond within seven working days. For more information, please refer to **Security Bug Bounty Porgram**.

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.

For the past few years, we have seen fruitful results that over 1.2 million customers have confidence in us, and the market share of our Synology DiskStation has increased across the globe, especially in the U.S., China, and countries in Europe. Synology will continue to improve our products and enhance our security solutions that can be tailored to unique needs.