Synology DSM critical OAuth flaw: patch when the update lands, or switch the package off now

20 November 2026 · 4 min read · blogs.iictp.org/synology-dsm-oauth-cve-2026-120382

Synology published security advisory Synology-SA-26:21 on 19 November 2026 for a critical vulnerability, CVE-2026-120382, in the OAuth API of DiskStation Manager (DSM) and in BeeStation OS. Synology says the flaw allows remote attackers to read or write arbitrary files and to cause denial of service. When we read the advisory, its status was "Ongoing", and some fixed releases were still scheduled rather than available.

TL;DR The short version

- Synology's advisory of 19 November 2026 covers CVE-2026-120382, a critical flaw (CVSS 9.8) in the OAuth API of DSM and BeeStation OS.
- It lets remote attackers read or write arbitrary files, and some fixed releases were still scheduled when we read the advisory.
- Find every Synology NAS you manage and deactivate the OAuth Service package now if you do not need it.

Read online, listen to it, or change the text size: https://blogs.iictp.org/synology-dsm-oauth-cve-2026-120382

What was reported

- Synology rates the flaw critical, with a CVSS 3 base score of 9.8 and a vector showing network access, no privileges and no user interaction required.
- The advisory classifies it as CWE-88, improper neutralisation of argument delimiters in a command, in the OAuth API.
- For DSM 7.4 the advisory says to upgrade to 7.4.1-90080-2 or above, and for DSM 7.3 to 7.3.2-86009-6 or above, both listed as scheduled for release by 20 November 2026.
- For DSM 7.2.2 and 7.2.1 the advisory lists the status as ongoing and recommends upgrading to 7.3.2-86009-6 or above. DSM 7.1 and BeeStation OS 1.5 are listed as ongoing.
- Synology lists APM, DSM Enterprise 1.0 and SRM 1.2 and 1.3 as not affected.
- The only mitigation the advisory gives is to deactivate the OAuth Service package.

What a practitioner should do

- Find every Synology NAS you are responsible for, including units in branch offices and home offices that hold company data, and record the DSM or BeeStation OS version on each.

- Check whether the OAuth Service package is installed and in use. If it is not needed, deactivate it now, as Synology advises, rather than waiting for the update.
- Remove direct internet exposure of the management interface where you can, and reach it through a VPN or other controlled access path instead.
- Install the fixed DSM release as soon as it appears for your version. Recheck the advisory, because its status and version table may change after publication.
- For units on versions still marked ongoing, plan the move to a supported release or keep the mitigation in place until a fix exists. Review file changes and logs on exposed units for anything you cannot explain.

The wider lesson

Storage appliances often sit outside the patching routine that covers servers and laptops, yet they hold some of the most valuable data an organisation has. An asset list that records versions and installed packages turns an advisory like this into a short, checkable task. That discipline belongs to the Infrastructure & Security domain of the TPBOK.

> Facts in this post were read from the sources listed below on 20 November 2026; this is a developing story or product and details may have changed since.

Sources and further reading

1. Synology. Synology-SA-26:21 DSM, BeeStation OS. Published 19 November 2026. synology.com/en-uk/security/advisory/Synology_SA_26_21

Published by IICTP, an independent technical credential body, on 20 November 2026. The current version of this post is at https://blogs.iictp.org/synology-dsm-oauth-cve-2026-120382. More guides: blogs.iictp.org.