Synology urges DSM updates after ransomware attacks on NAS devices



Synology reports ransomware attacks on NAS devices running outdated DSM versions, exploiting a flaw patched in December 2024. The vendor urges customers to update.

- Synology says attackers are exploiting a vulnerability in DiskStation Manager (DSM).
- The flaw was patched in December 2024; the targets are devices on outdated DSM versions.
- The vendor states the attacks aim to encrypt data and extort ransom.
- Synology is urging customers to update DSM.

Synology, the Taiwanese maker of Network Attached Storage (NAS) devices, has asked customers to update DiskStation Manager (DSM), the software that runs its devices, after observing ransomware attacks.

What the vendor reports

According to the company, threat actors are exploiting a vulnerability that it patched in December 2024. The attacks target devices still running outdated versions of DSM. In its statement, Synology said the aim of these attacks is to encrypt data and extort a ransom.

The source does not provide further technical detail, such as the CVE identifier, the number of affected devices or the identity of the attackers, so we do not speculate on them here.

Why it matters

The case is a reminder that a fix released long ago protects only the systems that have received it. NAS devices often hold file shares and backups, so a ransomware incident on one can affect both operations and recovery options.

What to do

Institutions using Synology NAS should confirm which DSM versions are deployed and bring them up to date using the vendor's guidance. Review the vendor's advisory for any further instructions specific to your models.

What to do now

1. Inventory all Synology NAS devices and record their DSM versions.
2. Update any device on an outdated DSM version, following Synology's guidance.
3. Review the vendor's advisory for model-specific instructions.
4. Check that backups held on or near NAS devices are intact and restorable.
5. Record the patching of these devices in your vulnerability management process.