



CVE-2021-26567

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-26567
State	PUBLIC
Assigner	security@synology.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-26 22:15:00 UTC
Updated	2023-06-26 19:20:00 UTC
Description	Stack-based buffer overflow vulnerability in frontend/main.c in faad2 before 2.2.7.1 allow local attackers to execute arbitrary

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Faad2 Project	Faad2	All	All	All	All
Application	Synology	Diskstation Manager	All	All	All	All
Application	Synology	Diskstation Manager	All	All	All	All
Operating System	Synology	Diskstation Manager Unified Controller	3.0	All	All	All
Operating System	Synology	Diskstation Manager Unified Controller	3.0	All	All	All
Hardware	Synology	Skynas	-	All	All	All
Hardware	Synology	Skynas	-	All	All	All
Hardware	Synology	Skynas	-	All	All	All
Operating System	Synology	Skynas Firmware	-	All	All	All
Operating System	Synology	Skynas Firmware	-	All	All	All
Hardware	Synology	Uc3200	-	All	All	All
Hardware	Synology	Uc3200	-	All	All	All
Hardware	Synology	Uc3200	-	All	All	All
Hardware	Synology	Vs960hd	-	All	All	All
Hardware	Synology	Vs960hd	-	All	All	All
Hardware	Synology	Vs960hd	-	All	All	All
Operating System	Synology	Vs960hd Firmware	-	All	All	All

Operating System	Synology	Vs960hd Firmware	-	All	All	All
------------------	----------	------------------	---	-----	-----	-----

References

Reference	Source	Link	Tags
Dynamically allocate file name buffers. · knik0/faad2@720f700 · GitHub	MISC	github.com	
Synology_SA_20_26 Synology Inc.	CONFIRM	www.synology.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

CVE.report and Source URL Uptime Status status.cve.report