



# CVE-2021-28799

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

## Summary

<b>CVE</b>	CVE-2021-28799
<b>State</b>	PUBLIC
<b>Assigner</b>	security@qnap.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-05-13 03:15:00 UTC
<b>Updated</b>	2023-11-14 19:26:00 UTC
<b>Description</b>	An improper authorization vulnerability has been reported to affect QNAP NAS running HBS 3 (Hybrid Backup Sync. ) If exp

## Risk And Classification

**EPSS:** 0.911460000 probability, percentile 0.996430000 (date 2026-04-01)

**CISA KEV:** Listed on 2022-03-31; due 2022-04-21; ransomware use Known

**Problem Types:** NVD-CWE-Other

## CISA Known Exploited Vulnerability

<b>Vendor</b>	QNAP
<b>Product</b>	Network Attached Storage (NAS)
<b>Name</b>	QNAP NAS Improper Authorization Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-28799">https://nvd.nist.gov/vuln/detail/CVE-2021-28799</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Qnap</a>	<a href="#">Hybrid Backup Sync</a>	All	All	All	All
Application	<a href="#">Qnap</a>	<a href="#">Qts</a>	4.3.3	All	All	All
Application	<a href="#">Qnap</a>	<a href="#">Qts</a>	4.3.4	All	All	All
Application	<a href="#">Qnap</a>	<a href="#">Qts</a>	4.3.6	All	All	All
Application	<a href="#">Qnap</a>	<a href="#">Qts</a>	4.5.2	All	All	All
Operating System	<a href="#">Qnap</a>	<a href="#">Qts</a>	4.3.6	All	All	All
Operating System	<a href="#">Qnap</a>	<a href="#">Qutsccloud</a>	All	All	All	All
Application	<a href="#">Qnap</a>	<a href="#">Quts Hero</a>	h4.5.1	All	All	All

Operating System	<a href="#">Qnap</a>	<a href="#">Quts Hero</a>	h4.5.1	All	All	All
References						
Reference	Source	Link	Tags			
Improper Authorization Vulnerability in HBS 3 Hybrid Backup Sync - Security Advisory   QNAP	MISC	<a href="http://www.qnap.com">www.qnap.com</a>				
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical			
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, an			
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="http://www.cisa.gov">www.cisa.gov</a>	kev			
Vendor Comments And Credit						
Discovery Credit						
<b>LEGACY: ZUSO ART</b>						
There are currently no legacy QID mappings associated with this CVE.						

© 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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**