



CVE-2021-28809

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

Summary

CVE	CVE-2021-28809
State	PUBLIC
Assigner	security@qnap.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-08 08:15:00 UTC
Updated	2021-07-12 16:37:00 UTC
Description	An improper access control vulnerability has been reported to affect certain legacy versions of HBS 3. If exploited, this vuln

Risk And Classification

Problem Types: CWE-284 | CWE-749 | CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qnap	Hybrid Backup Sync	All	All	All	All
Operating System	Qnap	Qts	4.3.3	-	All	All
Operating System	Qnap	Qts	4.3.4	-	All	All
Operating System	Qnap	Qts	4.3.6	-	All	All

References

Reference	Source	Link
ZDI-21-783 Zero Day Initiative	MISC	www.zerodayinitiative.com
Improper Access Control Vulnerability in Legacy HBS 3 (Hybrid Backup Sync) - Security Advisory QNAP	MISC	www.qnap.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Ta-Lun Yen of TXOne IoT/ICS Security Research Labs of Trend Micro working with Trend Micro's Zero Day Initiative

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](#)