

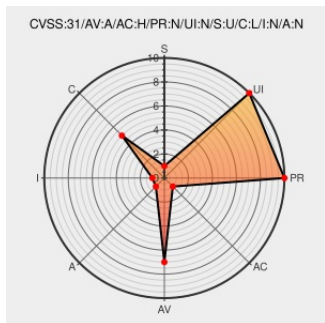


CVE-2021-28801

Published on: 06/11/2021 12:00:00 AM UTC

Last Modified on: 06/23/2021 02:24:00 PM UTC

CVE-2021-28801 - advisory for QSA-21-23

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Qss](#) from [Qnap](#) contain the following vulnerability:

An out-of-bounds read vulnerability has been reported to affect certain QNAP switches running QSS. If exploited, this vulnerability allows attackers to read sensitive information on the system. This issue affects: QNAP Systems Inc. QSS versions prior to 1.0.2 build 20210122 on QSW-M2108-2C; versions prior to 1.0.2 build 20210122 on QSW-M2108-2S; versions prior to 1.0.2 build 20210122 on QSW-

M2108R-2C.

CVE-2021-28801 has been assigned by [security@qnap.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [QNAP Systems Inc.](#) - QSS version < 1.0.2 build 20210122

Affected Vendor/Software: [QNAP Systems Inc.](#) - QSS version < 1.0.2 build 20210122

Affected Vendor/Software: [QNAP Systems Inc.](#) - QSS version < 1.0.2 build 20210122

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description

Tags

Link

Out-of-Bounds Read Vulnerability in QSS - Security Advisory | QNAP

[www.qnap.com](https://www.qnap.com/text/html)
text/html

 MISC www.qnap.com/zh-tw/security-advisory/qs-21-23

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qnap	Qss	All	All	All	All
Hardware 	Qnap	Qsw-m2108-2c	-	All	All	All
Hardware 	Qnap	Qsw-m2108-2s	-	All	All	All
Hardware 	Qnap	Qsw-m2108r-2c	-	All	All	All
cpe:2.3:a:qnap:qss:*:*:*:*:*:						
cpe:2.3:h:qnap:qsw-m2108-2c:*:*:*:*:*:						
cpe:2.3:h:qnap:qsw-m2108-2s:*:*:*:*:*:						
cpe:2.3:h:qnap:qsw-m2108r-2c:*:*:*:*:*:						

Discovery Credit

Qian Chen from Codesafe Team of Legendsec at Qi'anxin Group

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-28801 : An out-of-bounds read vulnerability has been reported to affect certain QNAP switches running QSS.... twitter.com/i/web/status/1...	2021-06-11 06:37:28
 /r/netcve	CVE-2021-28801	2021-06-11 07:41:24

[← Previous ID](#)

[Next ID →](#)

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](#)