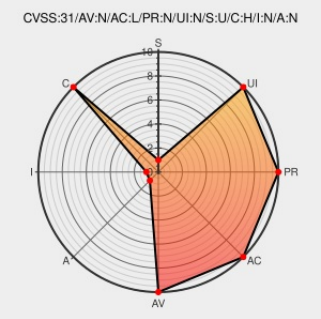
CVE-2020-24990

Published on: 10/28/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:37 PM UTC

CVE-2020-24990

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Q-sys Core Manager from Qsc contain the following vulnerability:

An issue was discovered in QSC Q-SYS Core Manager 8.2.1. By utilizing the TFTP service running on UDP port 69, a remote attacker can perform a directory traversal and obtain operating system files via a TFTP GET request, as demonstrated by reading /etc/passwd or /proc/version.

CVE-2020-24990 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

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
Q-SYS Core Manager	Vendor Advisory q-syshelp.qsc.com text/html	MISC q-syshelp.qsc.com/Content/Core_Manager/CoreManager_Overview.htm

QSC Q-SYS Core Manager 8.2.1 Directory Traversal ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/159699/QSC-Q-SYS-Core-Manager-8.2.1-Directory-Traversal.html
Full Disclosure: CVE-2020-24990 Q-SYS <= 8.2.1 TFTP Directory Traversal	Mailing List Third Party Advisory seclists.org text/html	MISC seclists.org/fulldisclosure/2020/Oct/30

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	Qsc	Q-sys Core Manager	8.2.1	All	All	All
Application	Qsc	Q-sys Core Manager	8.2.1	All	All	All

cpe:2.3:a:qsc:q-sys_core_manager:8.2.1:*:*:*:*:*:*:*

cpe:2.3:a:qsc:q-sys_core_manager:8.2.1:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→