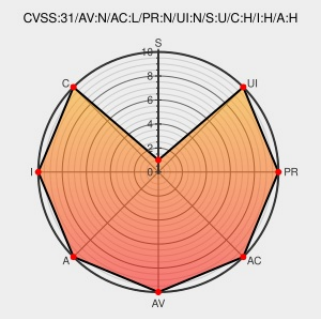
CVE-2020-2509

Published on: 04/16/2021 12:00:00 AM UTC

Last Modified on: 06/21/2021 04:56:00 PM UTC

CVE-2020-2509 - advisory for QSA-21-05

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



Certain versions of Qts from Qnap contain the following vulnerability:

A command injection vulnerability has been reported to affect QTS and QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary commands in a compromised application. We have already fixed this vulnerability in the following versions: QTS 4.5.2.1566 Build 20210202 and later QTS 4.5.1.1495 Build 20201123 and later QTS 4.3.6.1620 Build 20210322 and later QTS 4.3.4.1632 Build 20210324 and later QTS 4.3.3.1624 Build 20210416 and later QTS 4.2.6 Build 20210327 and later QuTS hero h4.5.1.1491 build 20201119 and later

CVE-2020-2509 has been assigned by security@qnap.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Command Injection Vulnerability in QTS and QuTS hero - Security		MISC www.qnap.com/en/security

Command Injection Vulnerability in QTS and QuTS hero - Security Advisory | QNAP	www.qnap.com text/html	MISC www.qnap.com/en/security-advisory/qsa-21-05

There are currently no QIDs associated with this CVE

Exploit/POC from Github

QNAP N-Day (Probably not CVE-2020-2509)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qnap	Qts	4.3.3.0174	All	All	All
Application	Qnap	Qts	4.3.3.0868	All	All	All
Application	Qnap	Qts	4.3.3.0998	All	All	All
Application	Qnap	Qts	4.3.3.1051	All	All	All
Application	Qnap	Qts	4.3.3.1098	All	All	All
Application	Qnap	Qts	4.3.3.1161	All	All	All
Application	Qnap	Qts	4.3.3.1252	All	All	All
Application	Qnap	Qts	4.3.3.1315	All	All	All
Application	Qnap	Qts	4.3.3.1386	All	All	All
Application	Qnap	Qts	4.3.3.1432	All	All	All
Operating System	Qnap	Qts	All	All	All	All
Operating System	Qnap	Qts	4.2.6	-	All	All
Operating System	Qnap	Qts	4.2.6	build_20170517	All	All
Operating System	Qnap	Qts	4.2.6	build_20190322	All	All
Operating System	Qnap	Qts	4.2.6	build_20190730	All	All
Operating System	Qnap	Qts	4.2.6	build_20190921	All	All
Operating System	Qnap	Qts	4.2.6	build_20191107	All	All
Operating System	Qnap	Qts	4.2.6	build_20200109	All	All
Operating System	Qnap	Qts	4.2.6	build_20200421	All	All

System						
Operating System	Qnap	Qts	4.2.6	build_20200611	All	All
Operating System	Qnap	Qts	4.2.6	build_20200821	All	All
Operating System	Qnap	Qts	4.3.4.0358	All	All	All
Operating System	Qnap	Qts	4.3.4.0358	beta1	All	All
Operating System	Qnap	Qts	4.3.4.0370	All	All	All
Operating System	Qnap	Qts	4.3.4.0370	beta1	All	All
Operating System	Qnap	Qts	4.3.4.0372	All	All	All
Operating System	Qnap	Qts	4.3.4.0372	beta1	All	All
Operating System	Qnap	Qts	4.3.4.0374	All	All	All
Operating System	Qnap	Qts	4.3.4.0374	beta1	All	All
Operating System	Qnap	Qts	4.3.4.0387	All	All	All
Operating System	Qnap	Qts	4.3.4.0387	beta2	All	All
Operating System	Qnap	Qts	4.3.4.0411	All	All	All
Operating System	Qnap	Qts	4.3.4.0416	All	All	All
Operating System	Qnap	Qts	4.3.4.0427	All	All	All
Operating System	Qnap	Qts	4.3.4.0434	All	All	All
Operating System	Qnap	Qts	4.3.4.0435	All	All	All
Operating System	Qnap	Qts	4.3.4.0451	All	All	All
Operating System	Qnap	Qts	4.3.4.0483	All	All	All
Operating System	Qnap	Qts	4.3.4.0486	All	All	All
Operating System	Qnap	Qts	4.3.4.0506	All	All	All
Operating System	Qnap	Qts	4.3.4.0516	All	All	All
Operating	Qnap	Qts	4.3.4.0526	All	All	All

System						
Operating System	Qnap	Qts	4.3.4.0551	All	All	All
Operating System	Qnap	Qts	4.3.4.0557	All	All	All
Operating System	Qnap	Qts	4.3.4.0561	All	All	All
Operating System	Qnap	Qts	4.3.4.0569	All	All	All
Operating System	Qnap	Qts	4.3.4.0593	All	All	All
Operating System	Qnap	Qts	4.3.4.0597	All	All	All
Operating System	Qnap	Qts	4.3.4.0604	All	All	All
Operating System	Qnap	Qts	4.3.4.0899	All	All	All
Operating System	Qnap	Qts	4.3.4.1029	All	All	All
Operating System	Qnap	Qts	4.3.4.1082	All	All	All
Operating System	Qnap	Qts	4.3.4.1190	All	All	All
Operating System	Qnap	Qts	4.3.4.1282	All	All	All
Operating System	Qnap	Qts	4.3.4.1368	All	All	All
Operating System	Qnap	Qts	4.3.4.1417	All	All	All
Operating System	Qnap	Qts	4.3.4.1463	All	All	All
Operating System	Qnap	Qts	4.3.6	-	All	All
Operating System	Qnap	Qts	4.3.6.0895	All	All	All
Operating System	Qnap	Qts	4.3.6.0907	All	All	All
Operating System	Qnap	Qts	4.3.6.0923	All	All	All
Operating System	Qnap	Qts	4.3.6.0944	All	All	All
Operating System	Qnap	Qts	4.3.6.0959	All	All	All
Operating System	Qnap	Qts	4.3.6.0979	All	All	All
Operating	Qnap	Qts	4.3.6.0993	All	All	All

System						
Operating System	Qnap	Qts	4.3.6.1013	All	All	All
Operating System	Qnap	Qts	4.3.6.1033	All	All	All
Operating System	Qnap	Qts	4.3.6.1070	All	All	All
Operating System	Qnap	Qts	4.3.6.1154	All	All	All
Operating System	Qnap	Qts	4.3.6.1218	All	All	All
Operating System	Qnap	Qts	4.3.6.1263	All	All	All
Operating System	Qnap	Qts	4.3.6.1286	All	All	All
Operating System	Qnap	Qts	4.3.6.1333	All	All	All
Operating System	Qnap	Qts	4.3.6.1411	All	All	All
Operating System	Qnap	Qts	4.3.6.1446	All	All	All
Operating System	Qnap	Qts	4.5.1	-	All	All
Operating System	Qnap	Qts	4.5.1.1456	All	All	All
Operating System	Qnap	Qts	4.5.1.1461	All	All	All
Operating System	Qnap	Qts	4.5.1.1465	All	All	All
Operating System	Qnap	Qts	4.5.1.1480	All	All	All
Operating System	Qnap	Qts	4.5.2	-	All	All
Application	Qnap	Quts Hero	All	All	All	All
Application	Qnap	Quts Hero	h4.5.1	-	All	All
Application	Qnap	Quts Hero	h4.5.1.1472	All	All	All
Operating System	Qnap	Quts Hero	All	All	All	All
Operating System	Qnap	Quts Hero	h4.5.1	-	All	All
Operating System	Qnap	Quts Hero	h4.5.1.1472	All	All	All

cpe:2.3:a:qnap:qts:4.3.3.0174:*:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.3.3.0868:*:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.3.3.0998:*:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.3.3.1051:*:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.3.3.1098:*:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.3.3.1161:*:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.3.3.1252:*:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.3.3.1315:*:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.3.3.1386:*:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.3.3.1432:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:*:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.2.6:-:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.2.6:build_20170517:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.2.6:build_20190322:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.2.6:build_20190730:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.2.6:build_20190921:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.2.6:build_20191107:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.2.6:build_20200109:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.2.6:build_20200421:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.2.6:build_20200611:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.2.6:build_20200821:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0358:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0358:beta1:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0370:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0370:beta1:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0372:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0372:beta1:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0374:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0374:beta1:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0387:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0387:beta2:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0411:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0416:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0427:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0434:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0435:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0451:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0483:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0486:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0506:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0516:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0526:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0551:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0557:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0561:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0569:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0593:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0597:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0604:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.0899:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.1029:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.1082:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.1190:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.1282:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.1368:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.1417:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.4.1463:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6:-:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6.0895:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6.0907:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6.0923:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6.0944:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6.0959:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6.0979:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6.0993:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6.1013:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6.1033:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6.1070:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6.1154:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6.1218:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6.1263:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6.1286:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6.1333:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6.1411:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.3.6.1446:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.5.1:-:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.5.1.1456:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.5.1.1461:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.5.1.1465:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.5.1.1480:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:4.5.2:-:*:*:*:*:*:*:

cpe:2.3:a:qnap:quts_hero:*:*:*:*:*:*:*:*:

cpe:2.3:a:qnap:quts_hero:h4.5.1:-:*:*:*:*:*:*:

cpe:2.3:a:qnap:quts_hero:h4.5.1.1472:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:quts_hero:*:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:quts_hero:h4.5.1:-:*:*:*:*:*:*:

cpe:2.3:o:qnap:quts_hero:h4.5.1.1472:*:*:*:*:*:*:*:

Discovery Credit

Omri Mallis, Yaniv Puyeski

Social Mentions

Source	Title	Posted (UTC)
@attritionorg	@threatpost re: bit.ly/3sIJoiB "tracked as CVE-2020-25099" then later "Tracked as CVE-2020-2509" and "The… twitter.com/i/web/status/1…	2021-04-02 00:22:56
@neerajaarora	#Legacy #QNAP #NAS Devices #Vulnerable to #Zero-Day Attack #CVE-2020-2509 #TheTimesOfIndia #TheHindu… twitter.com/i/web/status/1…	2021-04-02 06:24:30
@cybertzar	CVE-2020-2509 and CVE-2021-36195 are 2 bugs that, impact QNAP's model TS-231 network attached storage (NAS) hardwar… twitter.com/i/web/status/1…	2021-04-02 11:17:48
@cyberprotectgrp	"The bugs, tracked as CVE-2020-2509 and CVE-2021-36195, impact QNAP's model TS-231 network attached storage (NAS) h… twitter.com/i/web/status/1…	2021-04-02 12:04:33
@djbaird19	The bug (CVE-2020-2509) resides in the NAS web server (default TCP port 8080), according to researchers. Tracked a… twitter.com/i/web/status/1…	2021-04-02 12:26:09
@CSTOOL_io	@QNAP_nas NAS devices vulnerable to zero day attack: attacksrfc.cstool.io/cve/CVE-2020-2… #cybersecurity #homeoffice	2021-04-06 06:39:41
@UITSEC	?QNAP'ın NAS Cihazlarında Zero-Day Zafiyeti Tespit Edildi!! Bazı eski model nas cihazlarında CVE-2020-2509 ve CVE-… twitter.com/i/web/status/1…	2021-04-08 07:27:15
@CVEannounce	CVE-2020-2509, CVE-2020-36195, CVE-2018-19942, CVE-2021-3156, CVE-2020-2501 portswigger.net/daily-swig/qna…	2021-04-23 14:29:00
/r/netcve	CVE-2020-2509	2021-04-17 04:20:09
/r/qnap	With all the ransomware attacks, I highly recommend removing Multimedia Console and stop using QNAP software you don't need.	2021-04-23 05:27:42
/r/msp	Qlocker: Has anyone had to deal with this QNAP ransomware yet?	2021-04-23 13:23:36

← Previous ID

Next ID→