



CVE-2013-6277

Published on: 02/13/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:38 PM UTC

CVE-2013-6277

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

Certain versions of [Viocard 300](#) from [Qnap](#) contain the following vulnerability:

QNAP VioCard 300 has hardcoded RSA private keys.

CVE-2013-6277 has been assigned by [M](#) [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
firmware - ə - Free Online Firmware Unpacker, Scanner, Analyser - Firmware Genomics/Genome Project - Firmware Vulnerability and Backdoor Discovery - Firmware Mounting, Modification, Loading and Emulation - Embedded and Internet-of-Things Security	Exploit Third Party Advisory firmware.re text/html	MISC firmware.re/userixsec14/

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Hardware  	Qnap	Viocard 300	-	All	All	All
Hardware  	Qnap	Viocard 300	-	All	All	All
Operating System	Qnap	Viocard 300 Firmware	rs_b3722	All	All	All
Operating System	Qnap	Viocard 300 Firmware	rs_b4631	All	All	All
Operating System	Qnap	Viocard 300 Firmware	rs_b3722	All	All	All
Operating System	Qnap	Viocard 300 Firmware	rs_b4631	All	All	All
cpe:2.3:h:qnap:viocard_300:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:h:qnap:viocard_300:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:qnap:viocard_300_firmware:rs_b3722:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:qnap:viocard_300_firmware:rs_b4631:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:qnap:viocard_300_firmware:rs_b3722:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:qnap:viocard_300_firmware:rs_b4631:~::~~::~~::~~::~~::~~::~~::						

