



QNAP VioStor NVR OS Command Injection Vulnerability

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

Summary

CVE	CVE-2023-47565
State	RESERVED
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-12-21 00:00:00 UTC
Updated	2023-11-06 15:07:48 UTC
Description	QNAP VioStar NVR contains an OS command injection vulnerability that allows authenticated users to execute commands

Risk And Classification

EPSS: 0.867460000 probability, percentile 0.994290000 (date 2026-05-01)

CISA KEY: Listed on 2023-12-21; due 2024-01-11; ransomware use Unknown

CISA Known Exploited Vulnerability

Vendor	QNAP
Product	VioStor NVR
Name	QNAP VioStor NVR OS Command Injection Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	https://www.qnap.com/en/security-advisory/qs-a-23-48 ; https://nvd.nist.gov/vuln/detail/CVE-2023-47565

There are no known software configurations currently associated with this CVE in NVD or the CVE Program record.

References

Reference	Source	Link	Tags
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)