



# CVE-2021-42081

Published on: Not Yet Published

Last Modified on: 07/17/2023 06:30:00 PM UTC

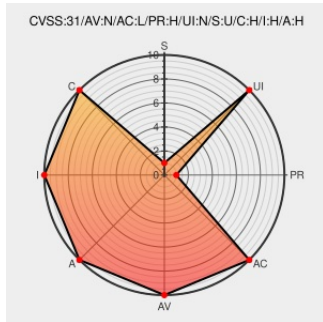
## CVE-2021-42081

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Quantastor](#) from [Osnexus](#) contain the following vulnerability:

An authenticated administrator is allowed to remotely execute arbitrary shell commands via the API.

CVE-2021-42081 has been assigned by csirt@divd.nl to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **OSNEXUS - QuantaStor** version < 6.0.0.355

CVSS3 Score: **7.2 - HIGH**

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

## CVE References

Description	Tags	Link
Redirecting...	<a href="#">csirt.divd.nl</a> <a href="#">text/html</a>	MISC <a href="#">csirt.divd.nl/CVE-2021-42081</a>
Software Defined Storage — OSNEXUS	<a href="#">www.osnexus.com</a> <a href="#">text/html</a>	MISC <a href="#">www.osnexus.com/products/software-defined-storage</a>
<a href="https://wbsec.nl/writeups/osnexus/">https://wbsec.nl/writeups/osnexus/</a>	<a href="#">www.wbsec.nl</a> <a href="#">text/html</a>	MISC <a href="#">www.wbsec.nl/osnexus</a>
DIVD /	<a href="#">www.divd.nl</a> <a href="#">text/html</a> <b>Inactive Link</b> <b>Not Archived</b>	MISC <a href="#">www.divd.nl/DIVD-2021-00020</a>

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

