



CVE-2017-9979

Published on: 08/28/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:56 PM UTC

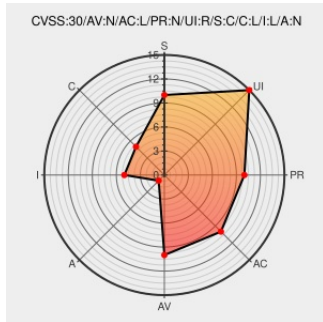
CVE-2017-9979

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

On the OSNEXUS QuantaStor v4 virtual appliance before 4.3.1, if the REST call invoked does not exist, an error will be triggered containing the invalid method previously invoked. The response sent to the user isn't sanitized in this case. An attacker can leverage this issue by including arbitrary HTML or JavaScript code as a parameter, aka XSS.

CVE-2017-9979 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE


CVE References

Description	Tags	Link
OSNEXUS QuantaStor 4 Information Disclosure ≈ Packet Storm	Exploit Third Party Advisory VDB Entry	MISC packetstormsecurity.com/files/143780/OSNEXUS-QuantaStor-4-Information-Disclosure.html

packetstormsecurity.com
[text/html](#)


404 Not Found

[Exploit](#)
[Third Party Advisory](#)
www.vvvsecurity.com
[text/html](#)
[Inactive Link](#) [Not Archived](#)

 MISC
www.vvvsecurity.com/advisories/vvvsecurity-advisory-2017-6943.txt

Full Disclosure: QuantaStor Software Define Storage mmultiple vulnerabilities

[Exploit](#)
[Mailing List](#)
[Third Party Advisory](#)
seclists.org
[text/html](#)

 FULLDISC 20170815 QuantaStor Software Define Storage mmultiple vulnerabilities

QuantaStor Software Defined Storage < 4.3.1 - Multiple Vulnerabilities - XML webapps Exploit

[Exploit](#)
[Third Party Advisory](#)
[VDB Entry](#)
www.exploit-db.com
[Proof of Concept](#)
[text/html](#)

 EXPLOIT-DB 42517

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	Osnexus	Quantastor	All	All	All	All

`cpe:2.3:a:osnexus:quantastor:*****:***:`

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#).

CVE.report and Source URL Uptime Status status.cve.report