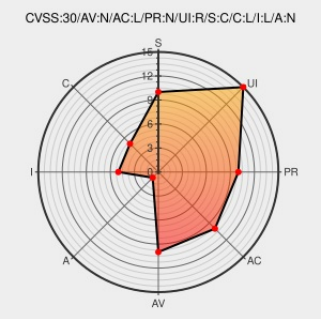
CVE-2017-9979

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 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

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→