



CVE-2018-5497

Published on: 01/24/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:46 PM UTC

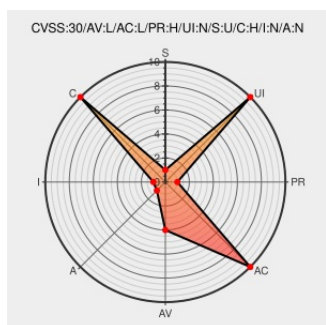
CVE-2018-5497

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Clustered Data Ontap](#) from [Netapp](#) contain the following vulnerability:

Clustered Data ONTAP versions prior to 9.1P16, 9.3P10 and 9.4P5 are susceptible to a vulnerability which discloses sensitive information to an unauthorized user.

CVE-2018-5497 has been assigned by security-alert@netapp.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **NetApp - Clustered Data ONTAP** version **Versions prior to 9.1P16, 9.3P10 and 9.4P5**

CVSS3 Score: **4.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
CVE-2018-5497 Sensitive Information Disclosure Vulnerability in Clustered Data ONTAP 9.x NetApp Product Security	Issue Tracking Vendor Advisory security.netapp.com	CONFIRM security.netapp.com/advisory/ntap-20190109-0001/

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	Netapp	Clustered Data Ontap	9.1	p10	All	All
Application	Netapp	Clustered Data Ontap	9.1	p11	All	All
Application	Netapp	Clustered Data Ontap	9.1	p12	All	All
Application	Netapp	Clustered Data Ontap	9.1	p13	All	All
Application	Netapp	Clustered Data Ontap	9.1	p14	All	All
Application	Netapp	Clustered Data Ontap	9.1	p15	All	All
Application	Netapp	Clustered Data Ontap	9.1	p2	All	All
Application	Netapp	Clustered Data Ontap	9.1	p3	All	All
Application	Netapp	Clustered Data Ontap	9.1	p4	All	All
Application	Netapp	Clustered Data Ontap	9.1	p5	All	All
Application	Netapp	Clustered Data Ontap	9.1	p6	All	All
Application	Netapp	Clustered Data Ontap	9.1	p7	All	All
Application	Netapp	Clustered Data Ontap	9.1	p8	All	All
Application	Netapp	Clustered Data Ontap	9.1	p9	All	All
Application	Netapp	Clustered Data Ontap	9.1	rc1	All	All
Application	Netapp	Clustered Data Ontap	9.3	p10	All	All
Application	Netapp	Clustered Data Ontap	9.4	p5	All	All
Application	Netapp	Clustered Data Ontap	9.1	p10	All	All
Application	Netapp	Clustered Data Ontap	9.1	p11	All	All
Application	Netapp	Clustered Data Ontap	9.1	p12	All	All
Application	Netapp	Clustered Data Ontap	9.1	p13	All	All
Application	Netapp	Clustered Data Ontap	9.1	p14	All	All
Application	Netapp	Clustered Data Ontap	9.1	p15	All	All
Application	Netapp	Clustered Data Ontap	9.1	p2	All	All
Application	Netapp	Clustered Data Ontap	9.1	p3	All	All
Application	Netapp	Clustered Data Ontap	9.1	p4	All	All
Application	Netapp	Clustered Data Ontap	9.1	p5	All	All

Application	Netapp	Clustered Data Ontap	9.1	p6	All	All
Application	Netapp	Clustered Data Ontap	9.1	p7	All	All
Application	Netapp	Clustered Data Ontap	9.1	p8	All	All
Application	Netapp	Clustered Data Ontap	9.1	p9	All	All
Application	Netapp	Clustered Data Ontap	9.1	rc1	All	All
Application	Netapp	Clustered Data Ontap	9.3	p10	All	All
Application	Netapp	Clustered Data Ontap	9.4	p5	All	All
Application	Netapp	Clustered Data Ontap	All	All	All	All
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p10:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p11:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p12:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p13:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p14:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p15:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p2:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p3:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p4:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p5:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p6:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p7:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p8:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p9:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:rc1:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p10:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.4:p5:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p10:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p11:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p12:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p13:*****:						
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p14:*****:						

cpe:2.3:a:netapp:clustered_data_ontap:9.1:p15:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p2:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p3:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p4:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p5:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p6:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p7:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p8:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.1:p9:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.1:rc1:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p10:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.4:p5:*****:
cpe:2.3:a:netapp:clustered_data_ontap:*****:

No vendor comments have been submitted for this CVE