



CVE-2020-8588

Published on: 02/03/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:59 PM UTC

CVE-2020-8588

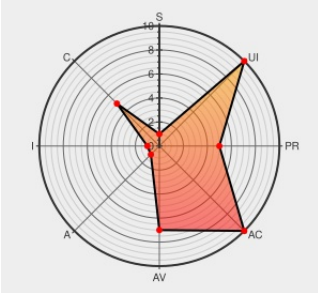
Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

CVSS:31/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N



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

Clustered Data ONTAP versions prior to 9.3P20 and 9.5P15 are susceptible to a vulnerability which could allow unauthorized tenant users to discover the existence of data on other Storage Virtual Machines (SVMs).

CVE-2020-8588 has been assigned by security-alert@netapp.com to track the vulnerability - currently rated as **LOW** severity.

CVSS3 Score: **3.5 - LOW**

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

CVSS2 Score: **2.7 - LOW**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
CVE-2020-8588 Sensitive Information Disclosure Vulnerability in Clustered Data ONTAP NetApp Product Security	Vendor Advisory security.netapp.com/text/html	CONFIRM security.netapp.com/advisory/ntap-20210201-0001/

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	All	All	All	All
Application	Netapp	Clustered Data Ontap	9.3	-	All	All
Application	Netapp	Clustered Data Ontap	9.3	p1	All	All
Application	Netapp	Clustered Data Ontap	9.3	p10	All	All
Application	Netapp	Clustered Data Ontap	9.3	p2	All	All
Application	Netapp	Clustered Data Ontap	9.3	p3	All	All
Application	Netapp	Clustered Data Ontap	9.3	p4	All	All
Application	Netapp	Clustered Data Ontap	9.3	p5	All	All
Application	Netapp	Clustered Data Ontap	9.3	p6	All	All
Application	Netapp	Clustered Data Ontap	9.3	p7	All	All
Application	Netapp	Clustered Data Ontap	9.3	p8	All	All
Application	Netapp	Clustered Data Ontap	9.3	p9	All	All
Application	Netapp	Clustered Data Ontap	9.3	rc1	All	All
Application	Netapp	Clustered Data Ontap	9.5	-	All	All
Application	Netapp	Clustered Data Ontap	9.5	p1	All	All
Operating System	Netapp	Clustered Data Ontap	9.5	p6	All	All
Operating System	Netapp	Clustered Data Ontap	9.5	p8	All	All
Operating System	Netapp	Clustered Data Ontap	9.5	p9	All	All
Application	Netapp	Clustered Data Ontap	All	All	All	All
Application	Netapp	Clustered Data Ontap	9.3	-	All	All
Application	Netapp	Clustered Data Ontap	9.3	p1	All	All
Application	Netapp	Clustered Data Ontap	9.3	p10	All	All
Application	Netapp	Clustered Data Ontap	9.3	p2	All	All
Application	Netapp	Clustered Data Ontap	9.3	p3	All	All
Application	Netapp	Clustered Data Ontap	9.3	p4	All	All
Application	Netapp	Clustered Data Ontap	9.3	p5	All	All
Application	Netapp	Clustered Data Ontap	9.3	p6	All	All

Application	Netapp	Clustered Data Ontap	9.3	p7	All	All
Application	Netapp	Clustered Data Ontap	9.3	p8	All	All
Application	Netapp	Clustered Data Ontap	9.3	p9	All	All
Application	Netapp	Clustered Data Ontap	9.3	rc1	All	All
Application	Netapp	Clustered Data Ontap	9.5	-	All	All
Application	Netapp	Clustered Data Ontap	9.5	p1	All	All
Operating System	Netapp	Clustered Data Ontap	9.5	p6	All	All
Operating System	Netapp	Clustered Data Ontap	9.5	p8	All	All
Operating System	Netapp	Clustered Data Ontap	9.5	p9	All	All
cpe:2.3:a:netapp:clustered_data_ontap:*:*:*:*:*:						
cpe:2.3:a:netapp:clustered_data_ontap:9.3:-:*:*:*:*:						
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p1:*:*:*:*:						
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p10:*:*:*:*:						
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p2:*:*:*:*:						
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p3:*:*:*:*:						
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p4:*:*:*:*:						
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p5:*:*:*:*:						
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p6:*:*:*:*:						
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p7:*:*:*:*:						
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p8:*:*:*:*:						
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p9:*:*:*:*:						
cpe:2.3:a:netapp:clustered_data_ontap:9.3:rc1:*:*:*:*:						
cpe:2.3:a:netapp:clustered_data_ontap:9.5:-:*:*:*:*:						
cpe:2.3:a:netapp:clustered_data_ontap:9.5:p1:*:*:*:*:						
cpe:2.3:o:netapp:clustered_data_ontap:9.5:p6:*:*:*:*:						
cpe:2.3:o:netapp:clustered_data_ontap:9.5:p8:*:*:*:*:						
cpe:2.3:o:netapp:clustered_data_ontap:9.5:p9:*:*:*:*:						
cpe:2.3:a:netapp:clustered_data_ontap:*:*:*:*:*:						
cpe:2.3:a:netapp:clustered_data_ontap:9.3:-:*:*:*:*:						

cpe:2.3:a:netapp:clustered_data_ontap:9.3:p1:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p10:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p2:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p3:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p4:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p5:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p6:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p7:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p8:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.3:p9:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.3:rc1:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.5:-:*****:
cpe:2.3:a:netapp:clustered_data_ontap:9.5:p1:*****:
cpe:2.3:o:netapp:clustered_data_ontap:9.5:p6:*****:
cpe:2.3:o:netapp:clustered_data_ontap:9.5:p8:*****:
cpe:2.3:o:netapp:clustered_data_ontap:9.5:p9:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)