



CVE-2018-5490

Published on: 08/03/2018 12:00:00 AM UTC

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

CVE-2018-5490

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Read-Only export policy rules are not correctly enforced in Clustered Data ONTAP 8.3 Release Candidate versions and therefore may allow more than "read-only" access from authenticated SMBv2 and SMBv3 clients. This behavior has been resolved in the GA release. Customers running prior release candidates (RCs) are requested to update their systems to the NetApp Data ONTAP 8.3 GA release.

CVE-2018-5490 has been assigned by security-alert@netapp.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **NetApp - Clustered Data ONTAP** version **8.3 Release Candidate versions**

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

Improper Handling of Export Policy Rules for SMBv2 and SMBv3 Clients
Vulnerability in Clustered Data ONTAP 8.3 Release Candidates | NetApp
Product Security

Vendor Advisory
security.netapp.com
text/html

 CONFIRM
security.netapp.com/advisory/ntap-
20150324-0001/

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	All	All	All	All

cpe:2.3:a:netapp:clustered_data_ontap:*****:

cpe:2.3:a:netapp:clustered_data_ontap:*****:

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](#)