

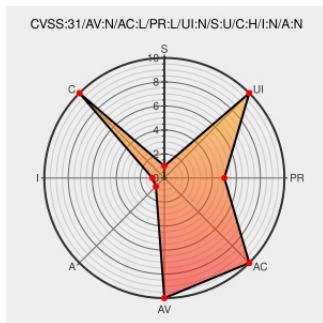


CVE-2020-7019

Published on: 08/18/2020 12:00:00 AM UTC

Last Modified on: 01/27/2023 08:50:00 PM UTC

CVE-2020-7019

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Elasticsearch](#) from [Elastic](#) contain the following vulnerability:

In Elasticsearch before 7.9.0 and 6.8.12 a field disclosure flaw was found when running a scrolling search with Field Level Security. If a user runs the same query another more privileged user recently ran, the scrolling search can leak fields that should be hidden. This could result in an attacker gaining additional permissions against a restricted index.

CVE-2020-7019 has been assigned by security@elastic.co to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Elastic** - **Elasticsearch** version **before 7.9.0**

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

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

CVE References

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

CVE-2020-7019 Elasticsearch Vulnerability in NetApp Products | NetApp Product Security

[security.netapp.com](#)
[text/html](#)

 **CONFIRM**
[security.netapp.com/advisory/ntap-20200827-0001/](#)

Elastic Stack 7.9.0 and 6.8.12 Security Update - Security Announcements - Discuss the Elastic Stack

[Vendor Advisory](#)
[discuss.elastic.co](#)
[text/html](#)

 **MISC** [discuss.elastic.co/t/elastic-stack-7-9-0-and-6-8-12-security-update/245456](#)

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.

Related QID Numbers

[690452](#) Free Berkeley Software Distribution (FreeBSD) Security Update for textproc/elasticsearch6 (fbca6863-e2ad-11ea-9d39-00a09858faf5)

[900438](#) Common Base Linux Mariner (CBL-Mariner) Security Update for rubygem-elasticsearch (6273)

[902011](#) Common Base Linux Mariner (CBL-Mariner) Security Update for rubygem-elasticsearch (6273-1)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Elastic	Elasticsearch	All	All	All	All
Application	Elastic	Elasticsearch	All	All	All	All
cpe:2.3:a:elastic:elasticsearch:*****:						
cpe:2.3:a:elastic:elasticsearch:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)