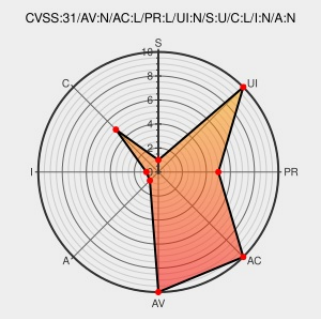
CVE-2021-22134

Published on: 03/08/2021 12:00:00 AM UTC

Last Modified on: 05/05/2021 01:28:00 PM UTC

CVE-2021-22134

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Elasticsearch from Elastic contain the following vulnerability:

A document disclosure flaw was found in Elasticsearch versions after 7.6.0 and before 7.11.0 when Document or Field Level Security is used. Get requests do not properly apply security permissions when executing a query against a recently updated document. This affects documents that have been updated and not yet refreshed in the index. This could result in the search disclosing the existence of documents and fields the attacker should not be able to view.

CVE-2021-22134 has been assigned by security@elastic.co to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Elastic** - **Elasticsearch** version **after 7.6.0 and before 7.11.0**

CVSS3 Score: 4.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	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
Elastic Stack 7.11.0 Security Update - Security Announcements - Discuss the Elastic Stack	Release Notes Vendor Advisory discuss.elastic.co text/html	MISC discuss.elastic.co/t/elastic-stack-7-11-0-security-update/265835
CVE-2021-22134 Elasticsearch Vulnerability in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20210430-0006/

Related QID Numbers

900490 Common Base Linux Mariner (CBL-Mariner) Security Update for rubygem-elasticsearch (6276)

982689 Java (maven) Security Update for org.elasticsearch:elasticsearch (GHSA-hwvv-438r-mhvj)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Elastic	Elasticsearch	All	All	All	All

cpe:2.3:a:elastic:elasticsearch:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Elasticsearch - CVE-2021-22134: discuss.elastic.co/t/elastic-stac…	2021-05-05 14:46:35

← Previous ID

Next ID→