



CVE-2021-22145

Published on: 07/21/2021 12:00:00 AM UTC

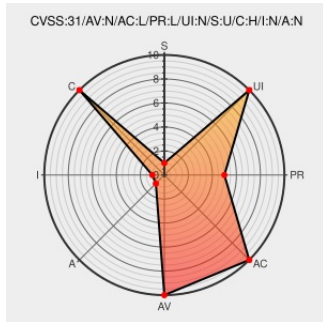
Last Modified on: 09/21/2021 06:17:00 PM UTC

CVE-2021-22145

Source: Mitre

Source: Nist

Print: PDF



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

A memory disclosure vulnerability was identified in Elasticsearch 7.10.0 to 7.13.3 error reporting. A user with the ability to submit arbitrary queries to Elasticsearch could submit a malformed query that would result in an error message returned containing previously used portions of a data buffer. This buffer could contain sensitive information such as Elasticsearch documents or authentication details.

CVE-2021-22145 has been assigned by security@elastic.co to track the vulnerability - currently rated as **MEDIUM** severity.

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
Elasticsearch 7.13.4 Security Update - Security Announcements - Discuss the Elastic Stack	discuss.elastic.co text/html	discuss.elastic.co/t/elasticsearch-7-13-4-security-update/279177

ElasticSearch 7.13.3 Memory Disclosure ≈ Packet Storm

[packetstormsecurity.com](https://packetstormsecurity.com/text/html)
text/html

MISC

packetstormsecurity.com/files/163648/ElasticSearch-7.13.3-Memory-Disclosure.html

July 2021 Elasticsearch Vulnerabilities in NetApp Products | NetApp Product Security

[security.netapp.com](https://security.netapp.com/text/html)
text/html

CONFIRM security.netapp.com/advisory/ntap-20210827-0006/

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

730234 Elasticsearch Memory Disclosure Vulnerability (ESA-2021-16)

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)
@CVEreport	CVE-2021-22145 : A memory disclosure vulnerability was identified in Elasticsearch 7.10.0 to 7.13.3 error reporting... twitter.com/i/web/status/1...	2021-07-21 12:42:52
/r/netcve	CVE-2021-22145	2021-07-21 13:38:13

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022 |

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