



CVE-2021-22146

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

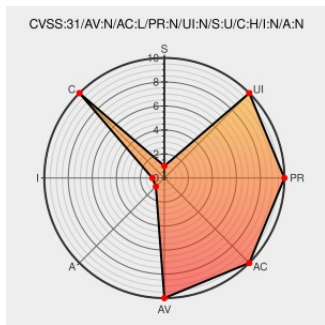
Last Modified on: 08/19/2021 10:15:00 AM UTC

CVE-2021-22146

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



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

All versions of Elastic Cloud Enterprise has the Elasticsearch “anonymous” user enabled by default in deployed clusters. While in the default setting the anonymous user has no permissions and is unable to successfully query any Elasticsearch APIs, an attacker could leverage the anonymous user to gain insight into certain details of a

deployed cluster.

CVE-2021-22146 has been assigned by security@elastic.co to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**


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

CVE References

Description	Tags	Link
Elasticsearch ECE 7.13.3 Database Disclosure ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/163655/Elasticsearch-


CVE-2021-22146 Elasticsearch Vulnerability in NetApp Products | NetApp Product Security

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

 CONFIRM security.netapp.com/advisory/ntap-20210819-0005/

Elastic Cloud Enterprise security update - Security Announcements - Discuss the Elastic Stack

[discuss.elastic.co
text/html](https://discuss.elastic.co/text/html)

 MISC discuss.elastic.co/t/elastic-cloud-enterprise-security-update/279180

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	Elastic	Elasticsearch	7.13.3	All	All	All
cpe:2.3:a:elastic:elasticsearch:7.13.3:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-22146 : All versions of Elastic Cloud Enterprise has the Elasticsearch “anonymous” user enabled by default... twitter.com/i/web/status/1...	2021-07-21 12:43:08
 /r/netcve	CVE-2021-22146	2021-07-21 13:38:14

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021   |

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