



# CVE-2020-7014

Published on: 06/03/2020 12:00:00 AM UTC

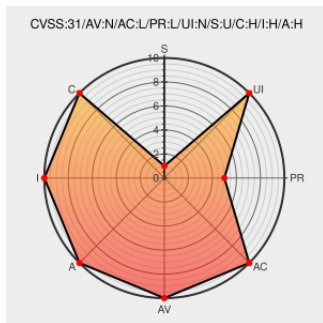
Last Modified on: 03/23/2021 11:23:54 PM UTC

## CVE-2020-7014

Source: Mitre

Source: Nist

Print: PDF



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

The fix for CVE-2020-7009 was found to be incomplete. Elasticsearch versions from 6.7.0 to 6.8.7 and 7.0.0 to 7.6.1 contain a privilege escalation flaw if an attacker is able to create API keys and also authentication tokens. An attacker who is able to generate an API key and an authentication token can perform a series of steps that result in an authentication token being generated with elevated privileges.

CVE-2020-7014 has been assigned by security@elastic.co to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Elastic - Elasticsearch** version **6.7.0 to 6.8.7 and 7.0.0 to 7.6.1**

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>LOW</b>	<b>SINGLE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>PARTIAL</b>	<b>PARTIAL</b>	<b>PARTIAL</b>

## CVE References

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

Security issues | Elastic

Vendor Advisory

N/A N/A

[www.elastic.co](http://www.elastic.co)

text/html

CVE-2020-7014 Elasticsearch Vulnerability in NetApp Products | NetApp Product Security

[security.netapp.com](http://security.netapp.com)

CONFIRM

text/html

[security.netapp.com/advisory/ntap-20200619-0003/](http://security.netapp.com/advisory/ntap-20200619-0003/)

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](mailto:comment@cve.report).

### Related QID Numbers

[900342](#) Common Base Linux Mariner (CBL-Mariner) Security Update for rubygem-elasticsearch (6272)

[982915](#) Java (maven) Security Update for org.elasticsearch:elasticsearch (GHSA-hqqv-9x3v-mp7w)

### Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Elastic</a>	<a href="#">Elasticsearch</a>	All	All	All	All
Application	<a href="#">Elastic</a>	<a href="#">Elasticsearch</a>	All	All	All	All
<code>cpe:2.3:a:elastic:elasticsearch:*****:</code>						
<code>cpe:2.3:a:elastic:elasticsearch:*****:</code>						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022 [T](#) [N](#) |

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](http://status.cve.report)