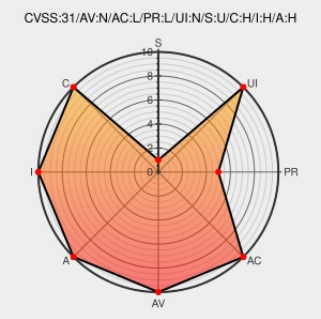
CVE-2020-7014

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
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link

Security issues | Elastic	Vendor Advisory www.elastic.co text/html	N/A N/A
CVE-2020-7014 Elasticsearch Vulnerability in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20200619-0003/

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	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→