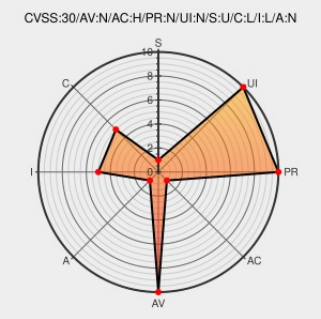
CVE-2017-12195

Published on: 07/27/2018 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:28:00 PM UTC

CVE-2017-12195

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Openshift Container Platform from Redhat contain the following vulnerability:

A flaw was found in all Openshift Enterprise versions using the openshift elasticsearch plugin. An attacker with knowledge of the given name used to authenticate and access Elasticsearch can later access it without the token, bypassing authentication. This attack also requires that the Elasticsearch be configured with an external route, and the data accessed is limited to the indices.

CVE-2017-12195 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Red Hat** - **OpenShift** version **= all**

CVSS3 Score: 4.8 - MEDIUM

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

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link

1501986 – (CVE-2017-12195) CVE-2017-12195 OpenShift Enterprise 3: authentication bypass for elasticsearch with external routes	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2017-12195
1501986 – (CVE-2017-12195) CVE-2017-12195 OpenShift Enterprise 3: authentication bypass for elasticsearch with external routes	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1501986
CVE-2017-12195 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2017-12195
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2017:3188
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2017:3389

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Openshift Container Platform	3.4	All	All	All
Application	Redhat	Openshift Container Platform	3.5	All	All	All
Application	Redhat	Openshift Container Platform	3.6	All	All	All
Application	Redhat	Openshift Container Platform	3.7	All	All	All
Application	Redhat	Openshift Container Platform	3.4	All	All	All
Application	Redhat	Openshift Container Platform	3.5	All	All	All
Application	Redhat	Openshift Container Platform	3.6	All	All	All
Application	Redhat	Openshift Container Platform	3.7	All	All	All

cpe:2.3:a:redhat:openshift_container_platform:3.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:3.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:3.6:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:3.7:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:3.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:3.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:3.6:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:3.7:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→