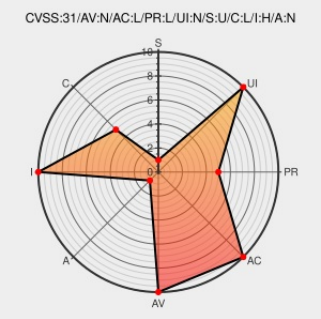
CVE-2021-31828

Published on: 05/06/2021 12:00:00 AM UTC

Last Modified on: 05/18/2021 01:26:00 PM UTC

CVE-2021-31828

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



Certain versions of Open Distro from Amazon contain the following vulnerability:

An SSRF issue in Open Distro for Elasticsearch (ODFE) before 1.13.1.0 allows an existing privileged user to enumerate listening services or interact with configured resources via HTTP requests exceeding the Alerting plugin's intended scope.

CVE-2021-31828 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.1 - HIGH

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

CVSS2 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
Support host deny list for Destinations by skkosuri-amzn · Pull Request #353 · opendistro-for-elasticsearch/alerting · GitHub	github.com text/html	CONFIRM github.com/opendistro-for-elasticsearch/alerting/pull/353
Version History - Open Distro for Elasticsearch Documentation	opendistro.github.io text/html	MISC opendistro.github.io/for-elasticsearch-docs/version-history/

CVE-2021-31828 - SSRF in Open Distro for ElasticSearch	rotem-bar.com text/html	MISC rotem-bar.com/ssrf-in-open-distro-for-elasticsearch-cve-2021-31828

There are currently no QIDs associated with this CVE

Exploit/POC from Github

PoC for exploiting CVE-2021-31828

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Amazon	Open Distro	All	All	All	All

cpe:2.3:a:amazon:open_distro:*:*:*:*:*:elasticsearch:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-31828 : An #SSRF issue in Open Distro for Elasticsearch ODFE before 1.13.1.0 allows an existing privileg… twitter.com/i/web/status/1…	2021-05-06 19:01:21
/r/netcve	CVE-2021-31828	2021-05-06 19:41:05

← Previous ID

Next ID→