

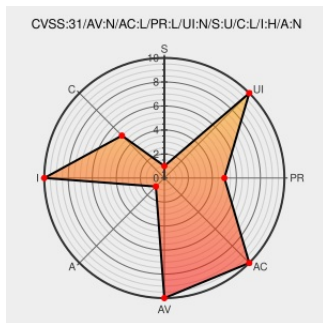


CVE-2021-31828

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 [M](#) 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/

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

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 →](#)