



CVE-2017-10906

Published on: 12/08/2017 12:00:00 AM UTC

Last Modified on: 08/04/2021 05:14:00 PM UTC

CVE-2017-10906

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Escape sequence injection vulnerability in Fluentd versions 0.12.29 through 0.12.40 may allow an attacker to change the terminal UI or execute arbitrary commands on the device via unspecified vectors.

CVE-2017-10906 has been assigned by [vultures@jpcert.or.jp](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Cloud Native Computing Foundation \(CNCF\)](#) - [Fluentd](#) version 0.12.29 through 0.12.40

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
fluentd/CHANGELOG.md at v0.12 · fluent/fluentd · GitHub	Issue Tracking Release Notes Third Party Advisory	CONFIRM github.com/fluent/fluentd/blob/v0.12/CHANGELOG.md#bug-fixes

Third Party Advisory
github.com
text/html

filter_parser: Fix dumped result for avoiding escape sequence injection by repeatedly · Pull Request #1733 · fluent/fluentd · GitHub

Issue Tracking
Patch
Third Party Advisory
github.com
text/html

 CONFIRM github.com/fluent/fluentd/pull/1733

JVNVU#95124098: Fluentd vulnerable to escape sequence injection

Issue Tracking
Third Party Advisory
VDB Entry
jvn.jp
text/xml

 MISC jvn.jp/en/vu/JVNVU95124098/index.html

Red Hat Customer Portal

Third Party Advisory
access.redhat.com
text/html

 REDHAT RHSA-2018:2225

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fluentd	Fluentd	0.12.29	All	All	All
Application	Fluentd	Fluentd	0.12.30	All	All	All
Application	Fluentd	Fluentd	0.12.31	All	All	All
Application	Fluentd	Fluentd	0.12.32	All	All	All
Application	Fluentd	Fluentd	0.12.33	All	All	All
Application	Fluentd	Fluentd	0.12.34	All	All	All
Application	Fluentd	Fluentd	0.12.35	All	All	All
Application	Fluentd	Fluentd	0.12.36	All	All	All
Application	Fluentd	Fluentd	0.12.37	All	All	All
Application	Fluentd	Fluentd	0.12.38	All	All	All
Application	Fluentd	Fluentd	0.12.39	All	All	All
Application	Fluentd	Fluentd	0.12.40	All	All	All
Application	Fluentd	Fluentd	0.12.29	All	All	All
Application	Fluentd	Fluentd	0.12.30	All	All	All
Application	Fluentd	Fluentd	0.12.31	All	All	All
Application	Fluentd	Fluentd	0.12.32	All	All	All
Application	Fluentd	Fluentd	0.12.33	All	All	All
Application	Fluentd	Fluentd	0.12.34	All	All	All

Application	Fluentd	Fluentd	0.12.35	All	All	All
Application	Fluentd	Fluentd	0.12.36	All	All	All
Application	Fluentd	Fluentd	0.12.37	All	All	All
Application	Fluentd	Fluentd	0.12.38	All	All	All
Application	Fluentd	Fluentd	0.12.39	All	All	All
Application	Fluentd	Fluentd	0.12.40	All	All	All
Application	Redhat	Openstack	13	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
cpe:2.3:a:fluentd:fluentd:0.12.29:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.30:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.31:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.32:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.33:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.34:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.35:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.36:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.37:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.38:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.39:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.40:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.29:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.30:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.31:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.32:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.33:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.34:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.35:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.36:*****:*						
cpe:2.3:a:fluentd:fluentd:0.12.37:*****:*						

cpe:2.3:a:fluentd:fluentd:0.12.38:*****:
cpe:2.3:a:fluentd:fluentd:0.12.39:*****:
cpe:2.3:a:fluentd:fluentd:0.12.40:*****:
cpe:2.3:a:redhat:openstack:13:*****:
cpe:2.3:a:redhat:openstack:13.0:*****:
cpe:2.3:a:redhat:openstack:13.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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](#)