



CVE-2021-41186

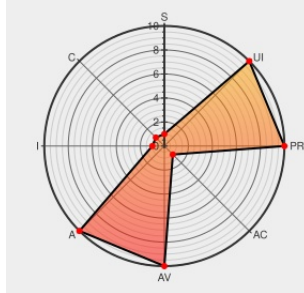
Published on: 10/29/2021 12:00:00 AM UTC

Last Modified on: 11/03/2021 12:11:00 AM UTC

CVE-2021-41186 - advisory for GHSA-hwhf-64mh-r662

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

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H



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

Fluentd collects events from various data sources and writes them to files to help unify logging infrastructure. The parser_apache2 plugin in Fluentd v0.14.14 to v1.14.1 suffers from a regular expression denial of service (ReDoS) vulnerability. A broken apache log with a certain pattern of string can spend too much time in a regular expression,

resulting in the potential for a DoS attack. This issue is patched in version 1.14.2 There are two workarounds available. Either don't use parser_apache2 for parsing logs (which cannot guarantee generated by Apache), or put patched version of parser_apache2.rb into /etc/fluent/plugin directory (or any other directories specified by the environment variable `FLUENT\_PLUGIN` or `--plugin` option of fluentd).

CVE-2021-41186 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: fluent - fluentd version $\geq 0.14.14$, $< 1.14.2$

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

NONE

NONE

PARTIAL

CVE References

Description	Tags	Link
fluentd/CHANGELOG.md at master · fluent/fluentd · GitHub	github.com text/html	MISC github.com/fluent/fluentd/blob/master/CHANGELOG.md#v1142
ReDoS vulnerability in parser_apache2 · Advisory · fluent/fluentd · GitHub	github.com text/html	CONFIRM github.com/fluent/fluentd/security/advisories/GHSA-hwhf-64mh-r662
Page not found · GitHub · GitHub	github.com text/html Inactive Link Not Archived	MISC github.com/github/securitylab-vulnerabilities/blob/52dc4a2a828c6dc24231967c2937ad92038184a9/vendor_reports/2021-102-fluent-fluentd.md

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.

Related QID Numbers

[900384](#) Common Base Linux Mariner (CBL-Mariner) Security Update for rubygem-fluentd (6279)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fluentd	Fluentd	All	All	All	All
cpe:2.3:a:fluentd:fluentd:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-41186 : Fluentd collects events from various data sources and writes them to files to help unify logging i... twitter.com/i/web/status/1...	2021-10-29 13:45:14
@LinInfoSec	Fluentd - CVE-2021-41186: github.com/fluent/fluentd...	2021-10-29 16:46:27
@0_exploit	CVE-2021-41186 dlvr.it/SBXnPr	2021-10-29 17:37:04
@threatmeter	CVE-2021-41186 Fluentd collects events from various data sources and writes them to files to help unify logging inf... twitter.com/i/web/status/1...	2021-10-30 07:09:57

[← 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](#)