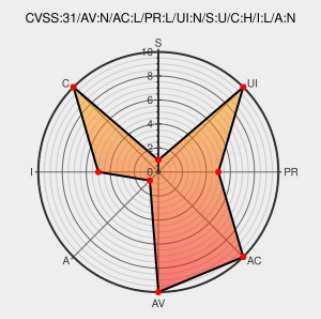
CVE-2021-43054

Published on: Not Yet Published

Last Modified on: 01/19/2022 03:11:00 PM UTC

CVE-2021-43054

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



Certain versions of Eftl from Tibco contain the following vulnerability:

The eFTL Server component of TIBCO Software Inc.'s TIBCO eFTL - Community Edition, TIBCO eFTL - Developer Edition, and TIBCO eFTL - Enterprise Edition contains an easily exploitable vulnerability that allows a low privileged attacker with network access to generate API tokens that can access any other channel with arbitrary permissions. Affected releases are TIBCO Software Inc.'s TIBCO eFTL - Community Edition: versions 6.7.2 and below, TIBCO eFTL - Developer Edition: versions 6.7.2 and below, and TIBCO eFTL - Enterprise Edition: versions 6.7.2 and below.

CVE-2021-43054 has been assigned by security@tibco.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **TIBCO Software Inc.** - **TIBCO eFTL - Community Edition** version **<= 6.7.2**

Affected Vendor/Software: **TIBCO Software Inc.** - **TIBCO eFTL - Developer Edition** version **<= 6.7.2**

Affected Vendor/Software: **TIBCO Software Inc.** - **TIBCO eFTL - Enterprise Edition** version **<= 6.7.2**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL | PARTIAL | PARTIAL

CVE References

Description	Tags	Link
Advisory | TIBCO Software	web.archive.org text/html Inactive Link Not Archived	CONFIRM www.tibco.com/services/support/advisories
TIBCO Security Advisory: January 11, 2022 - TIBCO eFTL - 2021-43054 | TIBCO Software	www.tibco.com text/html	CONFIRM www.tibco.com/support/advisories/2022/01/tibco-security-advisory-january-11-2022-tibco-eftl-2021-43054

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tibco	Eftl	All	All	All	All
Application	Tibco	Eftl	All	All	All	All
Application	Tibco	Eftl	All	All	All	All

cpe:2.3:a:tibco:eftl:*:*:*:*:community:*:*:*:

cpe:2.3:a:tibco:eftl:*:*:*:*:developer:*:*:*:

cpe:2.3:a:tibco:eftl:*:*:*:*:enterprise:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-43054 : The eFTL Server component of TIBCO Software Inc.'s TIBCO eFTL - Community Edition, TIBCO eFTL - De… twitter.com/i/web/status/1…	2022-01-11 18:31:04
/r/netcve	CVE-2021-43054	2022-01-11 19:38:38

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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