



CVE-2018-5434

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2018-5434
State	PUBLIC
Assigner	security@tibco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-13 13:29:00 UTC
Updated	2019-10-09 23:41:00 UTC
Description	The TIBCO Designer component of TIBCO Software Inc.'s TIBCO Runtime Agent, and TIBCO Runtime Agent for z/Linux c

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tibco	Runtime Agent	All	All	All	All
Application	Tibco	Runtime Agent	All	All	All	All

References

Reference	Source	Link	Tag
TIBCO Security Advisory: June 12, 2018 - TIBCO Runtime Agent - 2018-5434 TIBCO Software	CONFIRM	www.tibco.com	Ver
TIBCO Runtime Agent CVE-2018-5434 XML External Entity Injection Vulnerability	BID	www.securityfocus.com	Thi
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

Vendor Comments And Credit

Discovery Credit

LEGACY: TIBCO would like to extend its appreciation to Baker Hamilton at Bishop Fox for discovery of this vulnerability.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)