CVE-2012-2927

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2012-2927
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-05-22 15:55:02 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The TM Software Tempo plugin before 6.4.3.1, 6.5.x before 6.5.0.2, and 7.x before 7.0.3 for Atlassian JIRA does not prope

Risk And Classification

Primary CVSS: v2.0 4 from nvd@nist.gov

AV:N/AC:L/Au:S/C:N/I:N/A:P

Problem Types: CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:S/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Jira	-	All	All	All

Application	Tm Software	Tempo	2.2	All	All	All
Application	Tm Software	Tempo	2.3	All	All	All
Application	Tm Software	Tempo	2.3.1	All	All	All
Application	Tm Software	Tempo	2.4.1	All	All	All
Application	Tm Software	Tempo	2.5.1	All	All	All
Application	Tm Software	Tempo	2.6.1	All	All	All
Application	Tm Software	Tempo	2.7.1	All	All	All
Application	Tm Software	Tempo	2.8.1	All	All	All
Application	Tm Software	Tempo	4.0	All	All	All
Application	Tm Software	Tempo	4.0.1	All	All	All
Application	Tm Software	Tempo	4.1	All	All	All
Application	Tm Software	Tempo	4.2	All	All	All
Application	Tm Software	Tempo	4.3	All	All	All
Application	Tm Software	Tempo	4.4	All	All	All
Application	Tm Software	Tempo	4.4.2	All	All	All
Application	Tm Software	Tempo	4.5	All	All	All
Application	Tm Software	Tempo	4.5.2	All	All	All
Application	Tm Software	Tempo	5.0	All	All	All
Application	Tm Software	Tempo	5.1	All	All	All
Application	Tm Software	Tempo	5.1.1	All	All	All
Application	Tm Software	Tempo	5.2	All	All	All
Application	Tm Software	Tempo	5.2.1	All	All	All
Application	Tm Software	Tempo	5.2.2	All	All	All
Application	Tm Software	Tempo	5.2.3	All	All	All
Application	Tm Software	Tempo	5.3	All	All	All
Application	Tm Software	Tempo	5.3.1	All	All	All
Application	Tm Software	Tempo	5.3.2	All	All	All
Application	Tm Software	Tempo	5.3.3	All	All	All
Application	Tm Software	Tempo	5.3.3.1	All	All	All
Application	Tm Software	Tempo	5.4	All	All	All
Application	Tm Software	Tempo	5.4.1	All	All	All
Application	Tm Software	Tempo	5.4.2	All	All	All
Application	Tm Software	Tempo	6.0.0	All	All	All
Application	Tm Software	Tempo	6.0.1	All	All	All
Application	Tm Software	Tempo	6.0.2	All	All	All
Application	Tm Software	Tempo	6.0.3	All	All	All

Application	Tm Software	Tempo	6.1.0	All	All	All
Application	Tm Software	Tempo	6.1.1	jira42	All	All
Application	Tm Software	Tempo	6.2.0	All	All	All
Application	Tm Software	Tempo	6.2.1-jira42	All	All	All
Application	Tm Software	Tempo	6.2.2	jira42	All	All
Application	Tm Software	Tempo	6.2.3	jira42	All	All
Application	Tm Software	Tempo	6.2.4	jira42	All	All
Application	Tm Software	Tempo	6.2.5	jira42	All	All
Application	Tm Software	Tempo	6.2.6	jira42	All	All
Application	Tm Software	Tempo	6.2.7	jira42	All	All
Application	Tm Software	Tempo	6.3.1	jira42	All	All
Application	Tm Software	Tempo	6.4	jira42	All	All
Application	Tm Software	Tempo	6.4.2	All	All	All
Application	Tm Software	Tempo	6.5	All	All	All
Application	Tm Software	Tempo	7.0	All	All	All
Application	Tm Software	Tempo	7.0.0	rc1	All	All
Application	Tm Software	Tempo	7.0.0	rc2	All	All
Application	Tm Software	Tempo	7.0.2	All	All	All
Application	Tm Software	Tempo	All	All	All	All
Application	Tm Software	Tempo6.3.0	jira42	All	All	All
Application	Tm Software	Tempo6.3.2	jira42	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Security Advisory SA49166 - Atlassian JIRA Gliffy / Tempo Plugins XML Parsing Denial of Service Vulnerability - Secunia	af854a3a-2127-4
JIRA Security Advisory 2012-05-17 - JIRA 5.0 - Atlassian Documentation - Confluence	af854a3a-2127-4
osvdb.org/81993	af854a3a-2127-4
Multiple Atlassian Products XML Parsing Denial of Service Vulnerability	af854a3a-2127-4
IBM X-Force Exchange	af854a3a-2127-4
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**