CVE-2017-14589

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-14589
State	PUBLIC
Assigner	security@atlassian.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-13 15:29:00 UTC
Updated	2018-01-10 23:43:00 UTC
Description	It was possible for double OGNL evaluation in FreeMarker templates through Struts FreeMarker tags to occur. An attacker

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Bamboo	All	All	All	All
Application	Atlassian	Bamboo	All	All	All	All

References

Reference
Atlassian Bamboo CVE-2017-14589 Remote Code Execution Vulnerability
[BAM-18842] Remote code execution through OGNL double evaluation - CVE-2017-14589 - Create and track feature requests for Atlassian p
Bamboo Security Advisory 2017-12-13 - Atlassian Documentation
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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 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