



CVE-2017-18037

Published on: 02/02/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:55 PM UTC

CVE-2017-18037

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

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

The git repository tag rest resource in Atlassian Bitbucket Server from version 3.7.0 before 4.14.11 (the fixed version for 4.14.x), from version 5.0.0 before 5.0.9 (the fixed version for 5.0.x), from version 5.1.0 before 5.1.8 (the fixed version for 5.1.x), from version 5.2.0 before 5.2.6 (the fixed version for 5.2.x), from version 5.3.0 before 5.3.4 (the fixed version for 5.3.x), from version 5.4.0 before 5.4.2 (the fixed version for 5.4.x), from version 5.5.0 before 5.5.1 (the fixed version for 5.5.x) and before 5.6.0 allows remote attackers to read arbitrary files via a path traversal vulnerability through the name of a git tag.

CVE-2017-18037 has been assigned by [security@atlassian.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

 **CONFIRM**
jira.atlassian.com/browse/BSERV-10595

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Bitbucket	All	All	All	All
Application	Atlassian	Bitbucket	5.5.0	All	All	All
Application	Atlassian	Bitbucket	5.5.2	All	All	All
Application	Atlassian	Bitbucket	5.5.3	All	All	All
Application	Atlassian	Bitbucket	5.5.4	All	All	All
Application	Atlassian	Bitbucket	5.5.5	All	All	All
Application	Atlassian	Bitbucket	5.5.6	All	All	All
Application	Atlassian	Bitbucket	All	All	All	All
Application	Atlassian	Bitbucket	5.5.0	All	All	All
Application	Atlassian	Bitbucket	5.5.2	All	All	All
Application	Atlassian	Bitbucket	5.5.3	All	All	All
Application	Atlassian	Bitbucket	5.5.4	All	All	All
Application	Atlassian	Bitbucket	5.5.5	All	All	All
Application	Atlassian	Bitbucket	5.5.6	All	All	All
cpe:2.3:a:atlassian:bitbucket:*.*.*.*.*.*.*:						
cpe:2.3:a:atlassian:bitbucket:5.5.0:*.*.*.*.*.*.*:						
cpe:2.3:a:atlassian:bitbucket:5.5.2:*.*.*.*.*.*.*:						
cpe:2.3:a:atlassian:bitbucket:5.5.3:*.*.*.*.*.*.*:						
cpe:2.3:a:atlassian:bitbucket:5.5.4:*.*.*.*.*.*.*:						
cpe:2.3:a:atlassian:bitbucket:5.5.5:*.*.*.*.*.*.*:						
cpe:2.3:a:atlassian:bitbucket:5.5.6:*.*.*.*.*.*.*:						
cpe:2.3:a:atlassian:bitbucket:*.*.*.*.*.*.*:						
cpe:2.3:a:atlassian:bitbucket:5.5.0:*.*.*.*.*.*.*:						

cpe:2.3:a:atlassian:bitbucket:5.5.2:~::~::~:
cpe:2.3:a:atlassian:bitbucket:5.5.3:~::~::~:
cpe:2.3:a:atlassian:bitbucket:5.5.4:~::~::~:
cpe:2.3:a:atlassian:bitbucket:5.5.5:~::~::~:
cpe:2.3:a:atlassian:bitbucket:5.5.6:~::~::~:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →