



CVE-2017-18094

Published on: 03/22/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:54 PM UTC

CVE-2017-18094

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

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

Various resources in Atlassian Fisheye and Crucible before version 4.4.3 (the fixed version for 4.4.x) and 4.5.0 allow remote attackers with administrative privileges to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability through the base path setting of a configured file system repository.

CVE-2017-18094 has been assigned by [security@atlassian.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Atlassian](#) - **Fisheye and Crucible** version **prior to 4.4.3**

Affected Vendor/Software: [Atlassian](#) - **Fisheye and Crucible** version **prior to 4.5.0**

CVSS3 Score: **4.8 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

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

CVE References

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

 **CONFIRM**
jira.atlassian.com/browse/CRUC-8177

 **CONFIRM**
jira.atlassian.com/browse/FE-7010

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Crucible	All	All	All	All
Application	Atlassian	Crucible	4.5.0	All	All	All
Application	Atlassian	Crucible	All	All	All	All
Application	Atlassian	Crucible	4.5.0	All	All	All
Application	Atlassian	Fisheye	All	All	All	All
Application	Atlassian	Fisheye	4.5.0	All	All	All
Application	Atlassian	Fisheye	All	All	All	All
Application	Atlassian	Fisheye	4.5.0	All	All	All
cpe:2.3:a:atlassian:crucible:*****:						
cpe:2.3:a:atlassian:crucible:4.5.0:*****:						
cpe:2.3:a:atlassian:crucible:*****:						
cpe:2.3:a:atlassian:crucible:4.5.0:*****:						
cpe:2.3:a:atlassian:fisheye:*****:						
cpe:2.3:a:atlassian:fisheye:4.5.0:*****:						
cpe:2.3:a:atlassian:fisheye:*****:						
cpe:2.3:a:atlassian:fisheye:4.5.0:*****:						

Next ID→

© [CVE.report](#) 2023   |

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](#)