



CVE-2017-16861

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

Summary

CVE	CVE-2017-16861
State	PUBLIC
Assigner	security@atlassian.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-01 04:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	It was possible for double OGNL evaluation in certain redirect action and in WebWork URL and Anchor tags in JSP files to

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Crucible	All	All	All	All
Application	Atlassian	Crucible	All	All	All	All
Application	Atlassian	Fisheye	All	All	All	All
Application	Atlassian	Fisheye	All	All	All	All

References

Reference
[CRUC-8156] Remote code execution through OGNL double evaluation - CVE-2017-16861 - Create and track feature requests for Atlassian p
[FE-6991] Remote code execution through OGNL double evaluation - CVE-2017-16861 - Create and track feature requests for Atlassian prod
Page Not Found - Atlassian Documentation
Atlassian FishEye and Crucible CVE-2017-16861 Multiple Remote Code Execution Vulnerabilities
Fisheye and Crucible Security Advisory 2018-01-31 Crucible Server 4.8 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 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)