



CVE-2018-20240

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

Summary

CVE	CVE-2018-20240
State	PUBLIC
Assigner	security@atlassian.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-02-20 14:29:00 UTC
Updated	2019-02-26 17:16:00 UTC
Description	The administrative linker functionality in Atlassian Fisheye and Crucible before version 4.7.0 allows remote attackers to inject

Risk And Classification

Problem Types: CWE-79

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
[FE-7163] Stored XSS in administrative linker functionality through the href parameter - CVE-2018-20240 - Create and track feature requests for
Atlassian FishEye and Crucible Multiple Cross Site Scripting Vulnerabilities
[CRUC-8381] Stored XSS in administrative linker functionality through the href parameter - CVE-2018-20240 - Create and track feature requests for
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](#)