CVE-2017-14588

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-14588
State	PUBLIC
Assigner	security@atlassian.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-11 18:29:00 UTC
Updated	2020-11-25 14:15:00 UTC
Description	Various resources in Atlassian Fisheye and Crucible before version 4.4.2 allow remote attackers to inject arbitrary HTML or

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	Fisheye	All	All	All	All

References

Reference
[FE-6935] XSS in various resources through the dialog parameter - CVE-2017-14588 - Create and track feature requests for Atlassian product
[CRUC-8113] XSS in various resources through the dialog parameter - CVE-2017-14588 - Create and track feature requests for Atlassian pro
Atlassian FishEye and Crucible 'dialog' Parameter Multiple Cross Site Scripting Vulnerabilities
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report