CVE-2012-6342

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

Summary

CVE	CVE-2012-6342
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-13 14:55:00 UTC
Updated	2022-05-01 01:02:00 UTC
Description	Cross-site request forgery (CSRF) vulnerability in logout.action in Atlassian Confluence 3.4.6 allows remote attackers to hija

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Confluence	3.4.6	All	All	All
Application	Atlassian	Confluence	3.4.6	All	All	All
Application	Atlassian	Confluence Server	3.4.6	All	All	All

References

Reference
Atlassian Confluence 3.0 Cross Site Request Forgery ≈ Packet Storm
CVE-2012-6342: Atlassian Confluence - Multiple Cross-Site Request Forgery (CSRF) Vulnerabilities | HALOCK
[CONFSERVER-22784] logout.action is not protected against XSRF - CVE-2012-6342 - Create and track feature requests for Atlassian produ
20130116 Re: [CVE-ID REQUEST] Atlassian Confluence - Multiple Cross-Site Request Forgery (CSRF) Vulnerabilities
SecurityFocus
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