



CVE-2015-5285

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

Summary

CVE	CVE-2015-5285
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-29 20:59:00 UTC
Updated	2020-05-28 16:58:00 UTC
Description	CRLF injection vulnerability in Kallithea before 0.3 allows remote attackers to inject arbitrary HTTP headers and conduct HT

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kallithea-scm	Kallithea	All	All	All	All

References

Reference	Source	Link	Tags
Zero Science Lab » Kallithea 0.2.9 (came_from) HTTP Response Splitting Vulnerability	MISC	www.zeroscience.mk	Exploit
Kallithea · Security Notice CVE-2015-5285	CONFIRM	kallithea-scm.org	Exploit,
Kallithea 0.2.9 HTTP Response Splitting ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit
Kallithea 0.2.9 - 'came_from' HTTP Response Splitting - Multiple webapps Exploit	EXPLOIT-DB	www.exploit-db.com	Exploit
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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