



CVE-2016-3711

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

Summary

CVE	CVE-2016-3711
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-06-08 17:59:00 UTC
Updated	2023-02-12 23:19:00 UTC
Description	HAproxy in Red Hat OpenShift Enterprise 3.2 and OpenShift Origin allows local users to obtain the internal IP address of a

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Openshift	3.2	All	All	All
Application	Redhat	Openshift	3.2	All	All	All
Application	Redhat	Openshift Origin	-	All	All	All
Application	Redhat	Openshift Origin	-	All	All	All

References

Reference	Source	Link
haproxy obfuscated internal IP in routing cookie by pecameron · Pull Request #8334 · openshift/origin · GitHub	CONFIRM	github.com
Red Hat Customer Portal	REDHAT	access.redhat.c
CVE-2016-3711 - Red Hat Customer Portal	MISC	access.redhat.c
1322718 – (CVE-2016-3711) CVE-2016-3711 haproxy: Setting cookie containing internal IP address of a pod	MISC	bugzilla.redhat.
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)