



CVE-2018-10937

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2018-10937
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-11 16:29:00 UTC
Updated	2019-10-09 23:33:00 UTC
Description	A cross site scripting flaw exists in the tectonic-console component of Openshift Container Platform 3.11. An attacker with th

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All

References

Reference	Source	Link
1622372 – (CVE-2018-10937) CVE-2018-10937 tectonic-console: XSS Vulnerability in K8s API proxy	CONFIRM	bugz
Bug 1622372 - Require CSRF token on all proxied requests by spadgett · Pull Request #461 · openshift/console · GitHub	CONFIRM	github
Malformed Request	BID	www
Merge pull request #461 from spadgett/proxy · openshift/console@d566668 · GitHub	CONFIRM	github
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.i

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](#)