



CVE-2019-5925

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

Summary

CVE	CVE-2019-5925
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-12 22:29:00 UTC
Updated	2019-03-13 14:06:00 UTC
Description	Cross-site scripting vulnerability in Dradis Community Edition Dradis Community Edition v3.11 and earlier and Dradis Professional Edition v3.11 and earlier

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dradisframework	Dradis	All	All	All	All
Application	Dradisframework	Dradis	All	All	All	All

References

Reference	Source	Link
Security Reports Dradis Framework	MISC	dradisframework.com
JVN#40288903: Dradis Community Edition and Dradis Professional Edition vulnerable to cross-site scripting	JVN	jvn.jp
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.

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