



CVE-2015-2946

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

Summary

CVE	CVE-2015-2946
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-25 19:59:00 UTC
Updated	2016-12-03 03:07:00 UTC
Description	Stack-based buffer overflow in the Open CAD Format Council SXF common library before 3.30 allows remote attackers to e

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ocf	Sxf Common Library	All	All	All	All

References

Reference	Source	Link	Tags
JVN#93976566: SXF Common Library vulnerable to buffer overflow	JVN	jvn.jp	Vendor Advisory
JVNDB-2015-000068	JVNDB	jvndb.jvn.jp	Vendor Advisory
Japan Vulnerability Notes/Information from Open CAD Format Council	CONFIRM	jvn.jp	
SXF Common Library CVE-2015-2946 Buffer Overflow Vulnerability	BID	www.securityfocus.com	
トピックス 一般社団法人 OCF	CONFIRM	www.ocf.or.jp	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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