



CVE-2017-2187

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

Summary

CVE	CVE-2017-2187
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-09 16:29:00 UTC
Updated	2023-05-26 18:55:00 UTC
Description	Cross-site scripting vulnerability in WP Live Chat Support prior to version 7.0.07 allows remote attackers to inject arbitrary v

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	3cx	Live Chat	All	All	All	All
Application	Codecabin	Wp Live Chat Support	All	All	All	All

References

Reference	Source	Link	Tags
JVN#70951878: WordPress plugin "WP Live Chat Support" vulnerable to cross-site scripting	JVN	jvn.jp	Third Party
403 Forbidden	CONFIRM	plugins.trac.wordpress.org	Release
CVE Program record	CVE.ORG	www.cve.org	Canceled
NVD vulnerability detail	NVD	nvd.nist.gov	Canceled

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