



CVE-2020-13873

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

Summary

CVE	CVE-2020-13873
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-12 12:15:00 UTC
Updated	2021-05-20 19:18:00 UTC
Description	A SQL Injection vulnerability in get_topic_info() in sys/CODOF/Forum/Topic.php in Codoforum before 4.9 allows remote att

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Codologic	Codoforum	All	All	All	All

References

Reference
SmashITs · GitHub
SonarSource Blog
Latest Tech Stories topics - SonarSource Community
SonarSource on Twitter: "Critical #security vulnerabilities in Codoforum 4.8.7 explained: SQL injection, Path Traversal, and Persistent XSS #a
Codoforum 4.8.7: Critical Code Vulnerabilities Explained - Tech Stories - SonarSource Community
All topics CODOLOGIC
CVE Program record
NVD vulnerability detail

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](#)