

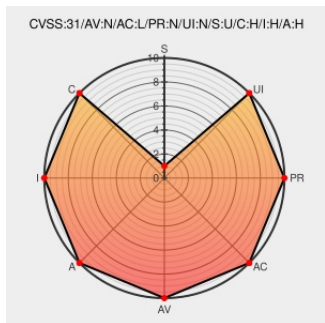


CVE-2021-46427

Published on: Not Yet Published

Last Modified on: 02/02/2022 05:18:00 PM UTC

CVE-2021-46427

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Simple Chatbot Application](#) from [Simple Chatbot Application Project](#) contain the following vulnerability:

An SQL Injection vulnerability exists in Sourcecodester Simple Chatbot Application 1.0 via the message parameter in Master.php.

CVE-2021-46427 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Simple Chatbot Application 1.0 SQL Injection - CXSecurity.com	cxsecurity.com text/html	MISC cxsecurity.com/issue/WLB-2022010092
Simple Chatbot Application 1.0 - 'message' Blind SQLi - PHP webapps Exploit	www.exploit-db.com Proof of Concept	MISC www.exploit-db.com/exploits/50673

text/html

CVE-2021-46427 - SQL-Injection-Bypass-Authentication+bonus=XSS-PHPSESSIONID-Hijacking

www.nu11secur1ty.com

text/html

MISC

www.nu11secur1ty.com/2022/01/cve-2021-46427-sql-injection-bypass.html

CVE-nu11secur1ty/vendors/oretnom23/2022/Simple ChatBot at main · nu11secur1ty/CVE-nu11secur1ty · GitHub

github.com

text/html

MISC

github.com/nu11secur1ty/CVE-nu11secur1ty/tree/main/vendors/oretnom23/2022/Simple%20ChatB

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Simple Chatbot Application Project	Simple Chatbot Application	1.0	All	All	All

cpe:2.3:a:simple_chatbot_application_project:simple_chatbot_application:1.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-46427 : An SQL Injection vulnerability exists in Sourcecodester Simple Chatbot Application 1.0 via the mes... twitter.com/i/web/status/1...	2022-01-27 19:05:41
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-46427 Description: An SQL Injection vulnerability exists in Sourcecodes... twitter.com/i/web/status/1...	2022-01-27 19:56:14
/r/netcve	CVE-2021-46427	2022-01-27 20:38:34

← Previous ID

Next ID→

© CVE.report 2023 |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)