



# CVE-2023-24656

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-24656
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-02-27 16:15:00 UTC
<b>Updated</b>	2023-03-01 00:18:00 UTC
<b>Description</b>	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the su

## Risk And Classification

**Problem Types:** CWE-89

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version
Application	Simple Customer Relationship Management System Project	Simple Customer Relationship Management System	1.0

## References

Reference	Source
<a href="http://www.sourcecodester.com/sites/default/files/download/oretnom23/php-scrm.zip">www.sourcecodester.com/sites/default/files/download/oretnom23/php-scrm.zip</a>	MISC
<a href="#">Simple Customer Relationship Management (CRM) System using PHP Free Source Code   Free Source Code Projects and Tutorials</a>	MISC
<a href="#">Simple Customer Relationship Management System v1.0 - SQL Injection Vulnerability · GitHub</a>	MISC
<a href="#">CVE Program record</a>	CVE.C
<a href="#">NVD vulnerability detail</a>	NVD

No vendor comments have been submitted for this CVE.

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)