



CVE-2022-2297

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

Summary

CVE	CVE-2022-2297
State	PUBLIC
Assigner	cna@vuldb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-12 17:15:00 UTC
Updated	2023-11-07 03:46:00 UTC
Description	A vulnerability, which was classified as critical, was found in SourceCodester Clinics Patient Management System 2.0. Affected versions are 2.0.0 through 2.0.1. The vulnerability is located in the upload.php file. The vulnerability is a buffer overflow that can be exploited to execute arbitrary code or cause a denial of service (DoS) attack. The vulnerability is caused by a lack of input validation and buffer overflow protection. The vulnerability is classified as critical because it can be exploited to execute arbitrary code or cause a denial of service (DoS) attack. The vulnerability is caused by a lack of input validation and buffer overflow protection.

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clinics Patient Management System Project	Clinics Patient Management System	2.0	All	All	All

References

Reference	Source	Link	Tags
CVE/POC.md at 8c6b66919be1bd66a54c16cc27cbdd9793221d3e · CyberThoth/CVE · GitHub		github.com	
CVE-2022-2297 SourceCodester Clinics Patient Management System unrestricted upload	MISC	vuldb.com	
CVE/POC.md at 8c6b66919be1bd66a54c16cc27cbdd9793221d3e · CyberThoth/CVE · GitHub	MISC	github.com	
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.

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