



CVE-2023-3806

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

Summary

CVE	CVE-2023-3806
State	PUBLIC
Assigner	cna@vuldb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-21 02:15:00 UTC
Updated	2023-11-07 04:19:00 UTC
Description	A vulnerability, which was classified as critical, was found in SourceCodester House Rental and Property Listing System 1.0. The vulnerability is located in the login.php file. The vulnerability is a remote denial of service (DoS) vulnerability. An attacker can exploit this vulnerability by sending a specially crafted request to the login.php file. This request will cause the application to crash and will result in a denial of service. The vulnerability is caused by a buffer overflow in the login.php file. The vulnerability is caused by a buffer overflow in the login.php file. The vulnerability is caused by a buffer overflow in the login.php file.

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Lang
Application	House Rental And Property Listing Php Project	House Rental And Property Listing Php	1.0	All	All	All

References

Reference	Source	Link
Login required	MISC	vuldb.com
CVE-2023-3806: SourceCodester House Rental and Property Listing System btn_functions.php unrestricted upload	MISC	vuldb.com
github.com/GZRsecurity/Cve-System/blob/main/House%20Rental%20and%20Prope...	MISC	github.com
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

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