



CVE-2008-4735

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

Summary

CVE	CVE-2008-4735
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-10-24 10:30:00 UTC
Updated	2017-09-29 01:32:00 UTC
Description	PHP remote file inclusion vulnerability in header.php in Concord Asset, Software, and Ticket system (CoAST) 0.95 allows re

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Coastal	Coast	0.95	All	All	All
Application	Coastal	Coast	0.95	All	All	All

References

Reference	Source	Link
CoAST 0.95 - 'sections_file' Remote File Inclusion - PHP webapps Exploit	EXPLOIT-DB	www.exploit-db.com/exploits/12345
CoAST "sections_file" File Inclusion Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com/advisories/4174
Concord Consortium CoAST 'header.php' Remote File Include Vulnerability	BID	www.securityfocus.com/bid/32841
CVE Program record	CVE.ORG	www.cve.org/CVE/nvd-2008-4735
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2008-4735

No vendor comments have been submitted for this CVE.

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

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