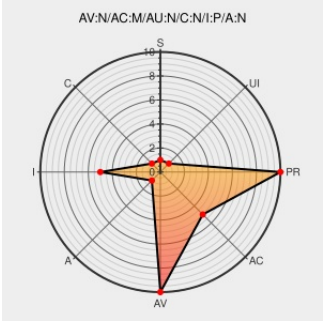
CVE-2005-4831

Published on: 12/31/2005 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

CVE-2005-4831

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Viewcvs from Viewcvs contain the following vulnerability:

viewcvs in ViewCVS 0.9.2 allows remote attackers to set the Content-Type header to arbitrary values via the content-type parameter, which can be leveraged for cross-site scripting (XSS) and other attacks, as demonstrated using (1) "text/html", or (2) "image/jpeg" with an image that is rendered as HTML by Internet Explorer, a different vulnerability than CVE-2004-1062. NOTE: it was later reported that 0.9.4 is also affected.

CVE-2005-4831 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
ViewCVS Source View Input Validation Vulnerability	Exploit, cve.report (archive), text/html	BID 12112
ViewCVS Input Validation Hole Permits Cross-Site Scripting Attacks - SecurityTracker	www.securitytracker.com, text/html	SECTRACK 1017704
SecurityFocus	www.securityfocus.com, text/html	BUGTRAQ 20070226 ViewCVS 0.9.4 issues
[Full-Disclosure] Two Vulnerabilities in ViewCVS	web.archive.org, text/html, Inactive Link, Not Archived	FULLDISC 20050101 Two Vulnerabilities in ViewCVS

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	Viewcvs	Viewcvs	0.9.2	All	All	All
Application	Viewcvs	Viewcvs	0.9.2	All	All	All

cpe:2.3:a:viewcvs:viewcvs:0.9.2:*:*:*:*:*:*:*:

cpe:2.3:a:viewcvs:viewcvs:0.9.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→