



CVE-2005-4550

Published on: 12/28/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:21 PM UTC

CVE-2005-4550

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Application Server Discussion Forum Portlet](#) from [Oracle](#) contain the following vulnerability:

The PORTAL schema in Oracle Application Server (OracleAS) Discussion Forum Portlet allows remote attackers to obtain the source code for arbitrary JSP and other files via a df_next_page parameter with a trailing null byte (%00).

CVE-2005-4550 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

CXSecurity - IDS

[securityreason.com](#)
[text/html](#)

[SREASON 297](#)

SecurityTracker.com Archives - OracleAS Discussion Forum Portlet Discloses Contents of Files on the System

[securitytracker.com](#)
[text/html](#)

[SECTRAK 1015406](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF oracle-forum-portlet-obtain-information\(23813\)](#)

'[Full-disclosure] SEC Consult SA-20051223-1 :: File Disclosure' - MARC

[marc.info](#)
[text/html](#)

[FULLDISC 20051223 SEC Consult SA-20051223-1 :: File Disclosure using df_next_page parameter in OracleAS Discussion Forum Portlet](#)

Oracle Application Server Discussion Forum Portlet Multiple Remote Vulnerabilities

[Exploit](#)
[cve.report \(archive\)](#)
[text/html](#)

[BID 16048](#)

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Application Server Discussion Forum Portlet	All	All	All	All
Application	Oracle	Application Server Discussion Forum Portlet	All	All	All	All
cpe:2.3:a:oracle:application_server_discussion_forum_portlet:*****:***:						
cpe:2.3:a:oracle:application_server_discussion_forum_portlet:*****:***:						

Next ID→