

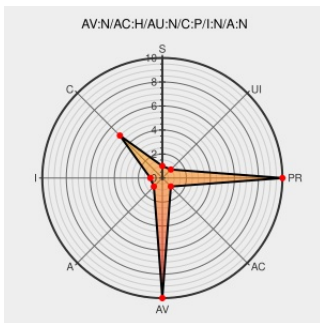


CVE-2004-1877

Published on: 03/30/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:09 PM UTC

CVE-2004-1877

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

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

The p_submit_url value in the sample login form in the Oracle 9i Application Server (9iAS) Single Sign-on Administrators Guide, Release 2(9.0.2) for Oracle SSO allows remote attackers to spoof the login page, which could allow users to inadvertently reveal their username and password.

CVE-2004-1877 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **2.6 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
'Problem with customized login pages for Oracle SSO' - MARC	marc.info text/html	BUGTRAQ 20040330 Problem with customized login pages for Oracle SSO
Oracle Single Sign-On Login Page Authentication Credential Disclosure Vulnerability	Patch Vendor Advisory cve.report (archive) text/html	BID 10009
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF oracle-sso-login-spoofing(15676)

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

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Application Server	1.0.2	All	All	All
Application	Oracle	Application Server	1.0.2.1s	All	All	All
Application	Oracle	Application Server	1.0.2.2	All	All	All
Application	Oracle	Application Server	1.0.2.2.2	All	All	All
Application	Oracle	Application Server	9.0.2	All	All	All
Application	Oracle	Application Server	9.0.2.0.0	All	All	All
Application	Oracle	Application Server	9.0.2.0.1	All	All	All
Application	Oracle	Application Server	9.0.2.1	All	All	All
Application	Oracle	Application Server	9.0.2.2	All	All	All
Application	Oracle	Application Server	9.0.2.3	All	All	All
Application	Oracle	Application Server	9.0.3	All	All	All
Application	Oracle	Application Server	9.0.3.1	All	All	All
Application	Oracle	Application Server	1.0.2	All	All	All
Application	Oracle	Application Server	1.0.2.1s	All	All	All
Application	Oracle	Application Server	1.0.2.2	All	All	All
Application	Oracle	Application Server	1.0.2.2.2	All	All	All
Application	Oracle	Application Server	9.0.2	All	All	All
Application	Oracle	Application Server	9.0.2.0.0	All	All	All
Application	Oracle	Application Server	9.0.2.0.1	All	All	All
Application	Oracle	Application Server	9.0.2.1	All	All	All
Application	Oracle	Application Server	9.0.2.2	All	All	All
Application	Oracle	Application Server	9.0.2.3	All	All	All
Application	Oracle	Application Server	9.0.3	All	All	All
Application	Oracle	Application Server	9.0.3.1	All	All	All
Application	Oracle	Http Server	8.1.7	All	All	All
Application	Oracle	Http Server	9.0.1	All	All	All
Application	Oracle	Http Server	9.2.0	All	All	All
Application	Oracle	Http Server	8.1.7	All	All	All
Application	Oracle	Http Server	9.0.1	All	All	All
Application	Oracle	Http Server	9.2.0	All	All	All

cpe:2.3:a:oracle:application_server:1.0.2:*****:
cpe:2.3:a:oracle:application_server:1.0.2.1s:*****:
cpe:2.3:a:oracle:application_server:1.0.2.2:*****:
cpe:2.3:a:oracle:application_server:1.0.2.2.2:*****:
cpe:2.3:a:oracle:application_server:9.0.2:*****:
cpe:2.3:a:oracle:application_server:9.0.2.0.0:*****:
cpe:2.3:a:oracle:application_server:9.0.2.0.1:*****:
cpe:2.3:a:oracle:application_server:9.0.2.1:*****:
cpe:2.3:a:oracle:application_server:9.0.2.2:*****:
cpe:2.3:a:oracle:application_server:9.0.2.3:*****:
cpe:2.3:a:oracle:application_server:9.0.3:*****:
cpe:2.3:a:oracle:application_server:9.0.3.1:*****:
cpe:2.3:a:oracle:application_server:1.0.2:*****:
cpe:2.3:a:oracle:application_server:1.0.2.1s:*****:
cpe:2.3:a:oracle:application_server:1.0.2.2:*****:
cpe:2.3:a:oracle:application_server:1.0.2.2.2:*****:
cpe:2.3:a:oracle:application_server:9.0.2:*****:
cpe:2.3:a:oracle:application_server:9.0.2.0.0:*****:
cpe:2.3:a:oracle:application_server:9.0.2.0.1:*****:
cpe:2.3:a:oracle:application_server:9.0.2.1:*****:
cpe:2.3:a:oracle:application_server:9.0.2.2:*****:
cpe:2.3:a:oracle:application_server:9.0.2.3:*****:
cpe:2.3:a:oracle:application_server:9.0.3:*****:
cpe:2.3:a:oracle:application_server:9.0.3.1:*****:
cpe:2.3:a:oracle:http_server:8.1.7:*****:
cpe:2.3:a:oracle:http_server:9.0.1:*****:
cpe:2.3:a:oracle:http_server:9.2.0:*****:
cpe:2.3:a:oracle:http_server:8.1.7:*****:

cpe:2.3:a:oracle:http_server:9.0.1:*****:

cpe:2.3:a:oracle:http_server:9.2.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)