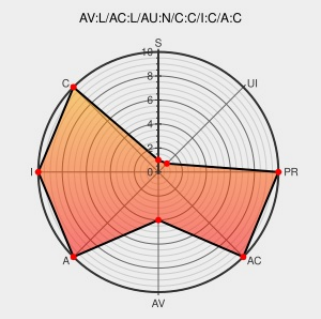
CVE-2004-1774

Published on: 08/31/2004 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1774

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



Certain versions of Application Server from Oracle contain the following vulnerability:

Buffer overflow in the SDO_CODE_SIZE procedure of the MD2 package (MDSYS.MD2.SDO_CODE_SIZE) in Oracle 10g before 10.1.0.2 Patch 2 allows local users to execute arbitrary code via a long LAYER parameter.

CVE-2004-1774 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Félicitations ! Votre domaine a bien été créé chez OVH !	Exploit, www.frsirt.com, text/html	MISC www.frsirt.com/exploits/20050413.OracleExploit.sql.php
[Full-Disclosure] Mailing List Charter	Vendor Advisory, lists.grok.org.uk, text/html, Inactive Link, Not Archived	FULLDISC 20040902 [SHATTER Team Security Alert] Multiple vulnerabilities in Oracle Database Server
Application Security Inc. - Securing Business by Securing Enterprise Applications	www.appsecinc.com, text/html	MISC www.appsecinc.com/resources/alerts/oracle/2004-0001/
SecuriTeam.com ™ - Multiple Vulnerabilities in Oracle Database Server (40 Issues)	Exploit, Patch, Vendor Advisory, www.securiteam.com	MISC www.securiteam.com/securitynews/5CP010KE0W.html

	text/html	
Page not found | Oracle	Vendor Advisory www.oracle.com application/pdf Inactive Link Not Archived	CONFIRM www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF oracle-mdsysmd2sdocodesize-bo(20078)
Oracle Database MDSYS.MD2.SDO_CODE_SIZE Buffer Overflow Vulnerability	Exploit Vendor Advisory cve.report (archive) text/html	BID 13145

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	10.1.0.2	All	All	All
Application	Oracle	Application Server	10.1.0.2	All	All	All
Application	Oracle	Oracle10g	enterprise_10.1.0.2	All	All	All
Application	Oracle	Oracle10g	personal_10.1.0.2	All	All	All
Application	Oracle	Oracle10g	standard_10.1.0.2	All	All	All
Application	Oracle	Oracle10g	enterprise_10.1.0.2	All	All	All
Application	Oracle	Oracle10g	personal_10.1.0.2	All	All	All
Application	Oracle	Oracle10g	standard_10.1.0.2	All	All	All

cpe:2.3:a:oracle:application_server:10.1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:application_server:10.1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:oracle10g:enterprise_10.1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:oracle10g:personal_10.1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:oracle10g:standard_10.1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:oracle10g:enterprise_10.1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:oracle10g:personal_10.1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:oracle10g:standard_10.1.0.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→