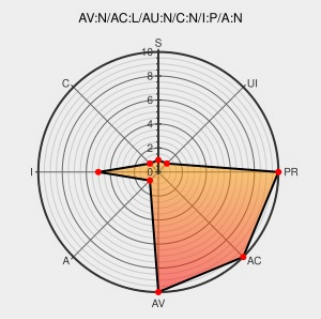
CVE-2005-2371

Published on: 07/26/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2371

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



Certain versions of Reports from Oracle contain the following vulnerability:

Directory traversal vulnerability in Oracle Reports 6.0, 6i, 9i, and 10g allows remote attackers to overwrite arbitrary files via (1) "..", (2) Windows drive letter (C:), and (3) absolute path sequences in the desname parameter. NOTE: this issue was probably fixed by REP06 in CPU Jan 2006, in which case it overlaps CVE-2006-0289.

CVE-2005-2371 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
SecurityTracker.com Archives - Oracle Reports Server 'desname' Parameter Lets Remote Authenticated Users Overwrite Files	securitytracker.com text/html	SECTRACK 1014524
Oracle Critical Patch Update - January 2006	web.archive.org text/html Inactive Link Not Archived	CONFIRM www.oracle.com/technetwork/topics/security/cpujan2006-082403.html
HP Oracle for Openview Multiple Vulnerabilities - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 18608
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF oracle-january2006-update(24321)

Oracle Reports Server DESName Remote File Overwrite Vulnerability	cve.report (archive) text/html	BID 14309
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060117 Oracle Reports - Overwrite any application server file via desname (fixed after 889 days)
No Description Provided	marc.info text/html	BUGTRAQ 20050719 Oracle Security Advisory: Overwrite any file via desname in Oracle Reports
Oracle Products Multiple Vulnerabilities and Security Issues - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 18493
Overwrite any file via desname in Oracle Reports	Vendor Advisory www.red-database-security.com text/html	MISC www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2006-0323

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Reports	10g	All	All	All
Application	Oracle	Reports	6.0	All	All	All
Application	Oracle	Reports	6i	All	All	All
Application	Oracle	Reports	9i	All	All	All
Application	Oracle	Reports	10g	All	All	All
Application	Oracle	Reports	6.0	All	All	All
Application	Oracle	Reports	6i	All	All	All
Application	Oracle	Reports	9i	All	All	All

cpe:2.3:a:oracle:reports:10g:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:reports:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:reports:6i:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:reports:9i:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:reports:10g:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:reports:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:reports:6i:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:reports:9i:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→