

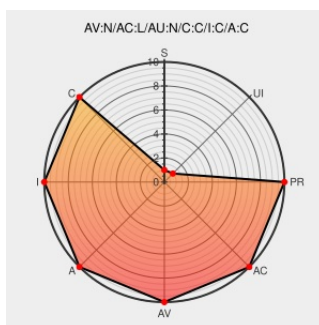


CVE-2003-1208

Published on: 12/03/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:44 PM UTC

CVE-2003-1208

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

Certain versions of [Oracle9i](#) from [Oracle](#) contain the following vulnerability:

Multiple buffer overflows in Oracle 9i 9 before 9.2.0.3 allow local users to execute arbitrary code by (1) setting the TIME_ZONE session parameter to a long value, or providing long parameters to the (2) NUMTOYMINTERVAL, (3) NUMTODSINTERVAL or (4) FROM_TZ functions.

CVE-2003-1208 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

nextgenss.com - This website is for sale! - nextgenss Resources and Information.

[Exploit](#)
[Patch](#)
[www.nextgenss.com](#)
[text/plain](#)

[MISC](#)
www.nextgenss.com/advisories/ora_from_tz.txt

US-CERT Vulnerability Note VU#240174

[Patch](#)
[Third Party Advisory](#)
[US Government Resource](#)
www.kb.cert.org
[text/html](#)

[CERT-VN VU#240174](#)

nextgenss.com - This website is for sale! - nextgenss Resources and Information.

[Exploit](#)
[www.nextgenss.com](#)
[text/plain](#)

[MISC](#)
www.nextgenss.com/advisories/ora_time_zone.txt

O-093: Oracle9i Database Buffer Overflow Vulnerabilities	Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	 CIAC O-093
nextgenss.com - This website is for sale! - nextgenss Resources and Information.	Exploit Patch www.nextgenss.com text/plain	 MISC www.nextgenss.com/advisories/ora_numtodsinterval.txt
US-CERT Vulnerability Note VU#399806	Patch Third Party Advisory US Government Resource www.kb.cert.org text/html	 CERT-VN VU#399806
nextgenss.com - This website is for sale! - nextgenss Resources and Information.	Exploit Patch www.nextgenss.com text/plain	 MISC www.nextgenss.com/advisories/ora_numtoyminterval.txt
No Description Provided	Exploit Patch Vendor Advisory www.osvdb.org Inactive Link Not Archived	 OSVDB 3840
US-CERT Vulnerability Note VU#846582	Patch Third Party Advisory US Government Resource www.kb.cert.org text/html	 CERT-VN VU#846582
No Description Provided	Exploit Patch Vendor Advisory www.osvdb.org Inactive Link Not Archived	 OSVDB 3839
US-CERT Vulnerability Note VU#819126	Patch Third Party Advisory US Government Resource www.kb.cert.org text/html	 CERT-VN VU#819126
Multiple Oracle Database Parameter/Statement Buffer Overflow Vulnerabilities	Exploit Patch Vendor Advisory cve.report (archive) text/html	 BID 9587
Secunia - Advisories - Oracle9i Database Multiple Buffer Overflow Vulnerabilities	Exploit Patch web.archive.org text/html	 SECUNIA 10805
No Description Provided	Exploit Vendor Advisory web.archive.org text/html Inactive Link Not Archived	 BUGTRAQ 20040205 Oracle Database 9i2 Interval Conversion Functions Buffer Overflow
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF oracle-multiple-function-bo(15060)

No Description Provided

Exploit

Patch

Vendor Advisory

www.osvdb.org

 OSVDB 3838

Inactive Link Not Archived

No Description Provided

Exploit

Patch

Vendor Advisory

www.osvdb.org

 OSVDB 3837

Inactive Link Not Archived

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	Oracle	Oracle9i	enterprise_9.0.1	All	All	All
Application	Oracle	Oracle9i	enterprise_9.2.0	All	All	All
Application	Oracle	Oracle9i	enterprise_9.2.0.1	All	All	All
Application	Oracle	Oracle9i	enterprise_9.2.0.2	All	All	All
Application	Oracle	Oracle9i	personal_9.0.1	All	All	All
Application	Oracle	Oracle9i	personal_9.2	All	All	All
Application	Oracle	Oracle9i	personal_9.2.0.1	All	All	All
Application	Oracle	Oracle9i	personal_9.2.0.2	All	All	All
Application	Oracle	Oracle9i	standard_9.0	All	All	All
Application	Oracle	Oracle9i	standard_9.0.1	All	All	All
Application	Oracle	Oracle9i	standard_9.0.1.2	All	All	All
Application	Oracle	Oracle9i	standard_9.0.1.3	All	All	All
Application	Oracle	Oracle9i	standard_9.0.1.4	All	All	All
Application	Oracle	Oracle9i	standard_9.0.2	All	All	All
Application	Oracle	Oracle9i	standard_9.2	All	All	All
Application	Oracle	Oracle9i	standard_9.2.0.1	All	All	All
Application	Oracle	Oracle9i	standard_9.2.0.2	All	All	All
Application	Oracle	Oracle9i	enterprise_9.0.1	All	All	All
Application	Oracle	Oracle9i	enterprise_9.2.0	All	All	All
Application	Oracle	Oracle9i	enterprise_9.2.0.1	All	All	All

Application	Oracle	Oracle9i	enterprise_9.2.0.2	All	All	All
Application	Oracle	Oracle9i	personal_9.0.1	All	All	All
Application	Oracle	Oracle9i	personal_9.2	All	All	All
Application	Oracle	Oracle9i	personal_9.2.0.1	All	All	All
Application	Oracle	Oracle9i	personal_9.2.0.2	All	All	All
Application	Oracle	Oracle9i	standard_9.0	All	All	All
Application	Oracle	Oracle9i	standard_9.0.1	All	All	All
Application	Oracle	Oracle9i	standard_9.0.1.2	All	All	All
Application	Oracle	Oracle9i	standard_9.0.1.3	All	All	All
Application	Oracle	Oracle9i	standard_9.0.1.4	All	All	All
Application	Oracle	Oracle9i	standard_9.0.2	All	All	All
Application	Oracle	Oracle9i	standard_9.2	All	All	All
Application	Oracle	Oracle9i	standard_9.2.0.1	All	All	All
Application	Oracle	Oracle9i	standard_9.2.0.2	All	All	All
cpe:2.3:a:oracle:oracle9i:enterprise_9.0.1:****:*:*:						
cpe:2.3:a:oracle:oracle9i:enterprise_9.2.0:****:*:*:						
cpe:2.3:a:oracle:oracle9i:enterprise_9.2.0.1:****:*:*:						
cpe:2.3:a:oracle:oracle9i:enterprise_9.2.0.2:****:*:*:						
cpe:2.3:a:oracle:oracle9i:personal_9.0.1:****:*:*:						
cpe:2.3:a:oracle:oracle9i:personal_9.2:****:*:*:						
cpe:2.3:a:oracle:oracle9i:personal_9.2.0.1:****:*:*:						
cpe:2.3:a:oracle:oracle9i:personal_9.2.0.2:****:*:*:						
cpe:2.3:a:oracle:oracle9i:standard_9.0:****:*:*:						
cpe:2.3:a:oracle:oracle9i:standard_9.0.1:****:*:*:						
cpe:2.3:a:oracle:oracle9i:standard_9.0.1.2:****:*:*:						
cpe:2.3:a:oracle:oracle9i:standard_9.0.1.3:****:*:*:						
cpe:2.3:a:oracle:oracle9i:standard_9.0.1.4:****:*:*:						
cpe:2.3:a:oracle:oracle9i:standard_9.0.2:****:*:*:						
cpe:2.3:a:oracle:oracle9i:standard_9.2:****:*:*:						
cpe:2.3:a:oracle:oracle9i:standard_9.2.0.1:****:*:*:						
cpe:2.3:a:oracle:oracle9i:standard_9.2.0.2:****:*:*:						

cpe:2.3:a:oracle:oracle9i:enterprise_9.0.1:*****:
cpe:2.3:a:oracle:oracle9i:enterprise_9.2.0:*****:
cpe:2.3:a:oracle:oracle9i:enterprise_9.2.0.1:*****:
cpe:2.3:a:oracle:oracle9i:enterprise_9.2.0.2:*****:
cpe:2.3:a:oracle:oracle9i:personal_9.0.1:*****:
cpe:2.3:a:oracle:oracle9i:personal_9.2:*****:
cpe:2.3:a:oracle:oracle9i:personal_9.2.0.1:*****:
cpe:2.3:a:oracle:oracle9i:personal_9.2.0.2:*****:
cpe:2.3:a:oracle:oracle9i:standard_9.0:*****:
cpe:2.3:a:oracle:oracle9i:standard_9.0.1:*****:
cpe:2.3:a:oracle:oracle9i:standard_9.0.1.2:*****:
cpe:2.3:a:oracle:oracle9i:standard_9.0.1.3:*****:
cpe:2.3:a:oracle:oracle9i:standard_9.0.1.4:*****:
cpe:2.3:a:oracle:oracle9i:standard_9.0.2:*****:
cpe:2.3:a:oracle:oracle9i:standard_9.2:*****:
cpe:2.3:a:oracle:oracle9i:standard_9.2.0.1:*****:
cpe:2.3:a:oracle:oracle9i:standard_9.2.0.2:*****:

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](#)