



[MITRE](#)
[NVD](#)
[CVE.ORG](#)
[JSON API](#)
[Print: PDF](#)

CVE	CVE-2011-0870
State	PUBLIC
Assigner	secalert_us@oracle.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-07-20 22:55:00 UTC
Updated	2014-10-04 04:34:00 UTC
Description	Unspecified vulnerability in the Schema Management component in Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 10.2.0.6, 10.2.0.7, 10.2.0.8, 10.2.0.9, 10.2.0.10, 10.2.0.11, 10.2.0.12, 10.2.0.13, 10.2.0.14, 10.2.0.15, 10.2.0.16, 10.2.0.17, 10.2.0.18, 10.2.0.19, 10.2.0.20, 10.2.0.21, 10.2.0.22, 10.2.0.23, 10.2.0.24, 10.2.0.25, 10.2.0.26, 10.2.0.27, 10.2.0.28, 10.2.0.29, 10.2.0.30, 10.2.0.31, 10.2.0.32, 10.2.0.33, 10.2.0.34, 10.2.0.35, 10.2.0.36, 10.2.0.37, 10.2.0.38, 10.2.0.39, 10.2.0.40, 10.2.0.41, 10.2.0.42, 10.2.0.43, 10.2.0.44, 10.2.0.45, 10.2.0.46, 10.2.0.47, 10.2.0.48, 10.2.0.49, 10.2.0.50, 10.2.0.51, 10.2.0.52, 10.2.0.53, 10.2.0.54, 10.2.0.55, 10.2.0.56, 10.2.0.57, 10.2.0.58, 10.2.0.59, 10.2.0.60, 10.2.0.61, 10.2.0.62, 10.2.0.63, 10.2.0.64, 10.2.0.65, 10.2.0.66, 10.2.0.67, 10.2.0.68, 10.2.0.69, 10.2.0.70, 10.2.0.71, 10.2.0.72, 10.2.0.73, 10.2.0.74, 10.2.0.75, 10.2.0.76, 10.2.0.77, 10.2.0.78, 10.2.0.79, 10.2.0.80, 10.2.0.81, 10.2.0.82, 10.2.0.83, 10.2.0.84, 10.2.0.85, 10.2.0.86, 10.2.0.87, 10.2.0.88, 10.2.0.89, 10.2.0.90, 10.2.0.91, 10.2.0.92, 10.2.0.93, 10.2.0.94, 10.2.0.95, 10.2.0.96, 10.2.0.97, 10.2.0.98, 10.2.0.99, 10.2.0.100, 10.2.0.101, 10.2.0.102, 10.2.0.103, 10.2.0.104, 10.2.0.105, 10.2.0.106, 10.2.0.107, 10.2.0.108, 10.2.0.109, 10.2.0.110, 10.2.0.111, 10.2.0.112, 10.2.0.113, 10.2.0.114, 10.2.0.115, 10.2.0.116, 10.2.0.117, 10.2.0.118, 10.2.0.119, 10.2.0.120, 10.2.0.121, 10.2.0.122, 10.2.0.123, 10.2.0.124, 10.2.0.125, 10.2.0.126, 10.2.0.127, 10.2.0.128, 10.2.0.129, 10.2.0.130, 10.2.0.131, 10.2.0.132, 10.2.0.133, 10.2.0.134, 10.2.0.135, 10.2.0.136, 10.2.0.137, 10.2.0.138, 10.2.0.139, 10.2.0.140, 10.2.0.141, 10.2.0.142, 10.2.0.143, 10.2.0.144, 10.2.0.145, 10.2.0.146, 10.2.0.147, 10.2.0.148, 10.2.0.149, 10.2.0.150, 10.2.0.151, 10.2.0.152, 10.2.0.153, 10.2.0.154, 10.2.0.155, 10.2.0.156, 10.2.0.157, 10.2.0.158, 10.2.0.159, 10.2.0.160, 10.2.0.161, 10.2.0.162, 10.2.0.163, 10.2.0.164, 10.2.0.165, 10.2.0.166, 10.2.0.167, 10.2.0.168, 10.2.0.169, 10.2.0.170, 10.2.0.171, 10.2.0.172, 10.2.0.173, 10.2.0.174, 10.2.0.175, 10.2.0.176, 10.2.0.177, 10.2.0.178, 10.2.0.179, 10.2.0.180, 10.2.0.181, 10.2.0.182, 10.2.0.183, 10.2.0.184, 10.2.0.185, 10.2.0.186, 10.2.0.187, 10.2.0.188, 10.2.0.189, 10.2.0.190, 10.2.0.191, 10.2.0.192, 10.2.0.193, 10.2.0.194, 10.2.0.195, 10.2.0.196, 10.2.0.197, 10.2.0.198, 10.2.0.199, 10.2.0.200, 10.2.0.201, 10.2.0.202, 10.2.0.203, 10.2.0.204, 10.2.0.205, 10.2.0.206, 10.2.0.207, 10.2.0.208, 10.2.0.209, 10.2.0.210, 10.2.0.211, 10.2.0.212, 10.2.0.213, 10.2.0.214, 10.2.0.215, 10.2.0.216, 10.2.0.217, 10.2.0.218, 10.2.0.219, 10.2.0.220, 10.2.0.221, 10.2.0.222, 10.2.0.223, 10.2.0.224, 10.2.0.225, 10.2.0.226, 10.2.0.227, 10.2.0.228, 10.2.0.229, 10.2.0.230, 10.2.0.231, 10.2.0.232, 10.2.0.233, 10.2.0.234, 10.2.0.235, 10.2.0.236, 10.2.0.237, 10.2.0.238, 10.2.0.239, 10.2.0.240, 10.2.0.241, 10.2.0.242, 10.2.0.243, 10.2.0.244, 10.2.0.245, 10.2.0.246, 10.2.0.247, 10.2.0.248, 10.2.0.249, 10.2.0.250, 10.2.0.251, 10.2.0.252, 10.2.0.253, 10.2.0.254, 10.2.0.255, 10.2.0.256, 10.2.0.257, 10.2.0.258, 10.2.0.259, 10.2.0.260, 10.2.0.261, 10.2.0.262, 10.2.0.263, 10.2.0.264, 10.2.0.265, 10.2.0.266, 10.2.0.267, 10.2.0.268, 10.2.0.269, 10.2.0.270, 10.2.0.271, 10.2.0.272, 10.2.0.273, 10.2.0.274, 10.2.0.275, 10.2.0.276, 10.2.0.277, 10.2.0.278, 10.2.0.279, 10.2.0.280, 10.2.0.281, 10.2.0.282, 10.2.0.283, 10.2.0.284, 10.2.0.285, 10.2.0.286, 10.2.0.287, 10.2.0.288, 10.2.0.289, 10.2.0.290, 10.2.0.291, 10.2.0.292, 10.2.0.293, 10.2.0.294, 10.2.0.295, 10.2.0.296, 10.2.0.297, 10.2.0.298, 10.2.0.299, 10.2.0.300, 10.2.0.301, 10.2.0.302, 10.2.0.303, 10.2.0.304, 10.2.0.305, 10.2.0.306, 10.2.0.307, 10.2.0.308, 10.2.0.309, 10.2.0.310, 10.2.0.311, 10.2.0.312, 10.2.0.313, 10.2.0.314, 10.2.0.315, 10.2.0.316, 10.2.0.317, 10.2.0.318, 10.2.0.319, 10.2.0.320, 10.2.0.321, 10.2.0.322, 10.2.0.323, 10.2.0.324, 10.2.0.325, 10.2.0.326, 10.2.0.327, 10.2.0.328, 10.2.0.329, 10.2.0.330, 10.2.0.331, 10.2.0.332, 10.2.0.333, 10.2.0.

Problem Types: NVD-CWE-noinfo

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Database Server	10.1.0.5	All	All	All
Application	Oracle	Database Server	10.2.0.3	All	All	All
Application	Oracle	Database Server	10.2.0.4	All	All	All
Application	Oracle	Database Server	10.2.0.5	All	All	All
Application	Oracle	Database Server	11.1.0.7	All	All	All
Application	Oracle	Database Server	11.2.0.1	All	All	All
Application	Oracle	Database Server	11.2.0.2	All	All	All
Application	Oracle	Database Server	10.1.0.5	All	All	All
Application	Oracle	Database Server	10.2.0.3	All	All	All
Application	Oracle	Database Server	10.2.0.4	All	All	All
Application	Oracle	Database Server	10.2.0.5	All	All	All
Application	Oracle	Database Server	11.1.0.7	All	All	All
Application	Oracle	Database Server	11.2.0.1	All	All	All
Application	Oracle	Database Server	11.2.0.2	All	All	All
Application	Oracle	Enterprise Manager Grid Control	10.1.0.6	All	All	All
Application	Oracle	Enterprise Manager Grid Control	10.2.0.5	All	All	All
Application	Oracle	Enterprise Manager Grid Control	10.1.0.6	All	All	All

Application	Oracle	Enterprise Manager Grid Control	10.2.0.5	All	All	All
-------------	--------	---------------------------------	----------	-----	-----	-----

References					
Reference	Source	Link	Tags		
US-CERT Technical Cyber Security Alert TA11-201A -- Oracle Updates for Multiple Vulnerabilities	CERT	www.us-cert.gov	US G		
Gentoo Linux Documentation -- IcedTea JDK: Multiple vulnerabilities	GENTOO	security.gentoo.org			
Oracle Critical Patch Update - July 2011	CONFIRM	www.oracle.com	Patch		
CVE Program record	CVE.ORG	www.cve.org	canon		
NVD vulnerability detail	NVD	nvd.nist.gov	canon		

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](http://cve.report) 2026 |

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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report