



CVE-2011-4358

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

Summary

CVE	CVE-2011-4358
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-07-17 22:55:00 UTC
Updated	2014-10-10 04:43:00 UTC
Description	Unspecified vulnerability in Oracle GlassFish Enterprise Server 3.0.1 and 3.1.1 allows remote attackers to affect confidentiality

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Sun Glassfish Enterprise Server	3.0.1	All	All	All
Application	Oracle	Sun Glassfish Enterprise Server	3.1.1	All	All	All
Application	Oracle	Sun Glassfish Enterprise Server	3.0.1	All	All	All
Application	Oracle	Sun Glassfish Enterprise Server	3.1.1	All	All	All

References

Reference	Source	Link
Sun GlassFish Enterprise Server Bug Lets Remote Users Partially Access and Modify Data - SecurityTracker	SECTRACK	www.securitytr
Support / Security / Advisories // MDVSA-2013:150 Mandriva	MANDRIVA	www.mandriva
Oracle Critical Patch Update - July 2012	CONFIRM	www.oracle.co
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [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](#).

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