



CVE-2015-0396

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

Summary

CVE	CVE-2015-0396
State	PUBLIC
Assigner	secalert_us@oracle.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-01-21 18:59:00 UTC
Updated	2017-09-08 01:29:00 UTC
Description	Unspecified vulnerability in the Oracle GlassFish Server component in Oracle Fusion Middleware 3.0.1 and 3.1.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory consumption) via a crafted SOAP request, as demonstrated by the SOAPAction header. The vulnerability is due to the way the SOAPAction header is processed. A remote attacker can send a SOAP request with a crafted SOAPAction header that causes the server to execute arbitrary code or cause a denial of service (memory consumption). The vulnerability is due to the way the SOAPAction header is processed. A remote attacker can send a SOAP request with a crafted SOAPAction header that causes the server to execute arbitrary code or cause a denial of service (memory consumption).

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Fusion Middleware	3.0.1	All	All	All
Application	Oracle	Fusion Middleware	3.1.2	All	All	All
Application	Oracle	Fusion Middleware	3.0.1	All	All	All
Application	Oracle	Fusion Middleware	3.1.2	All	All	All

References

Reference	Source	Link
IBM X-Force Exchange	XF	eX
Oracle GlassFish Server Flaw Lets Remote Users Partially Access Data, Modify Data, and Deny Service - SecurityTracker	SECTrack	w
Oracle GlassFish Server CVE-2015-0396 Remote Security Vulnerability	BID	w
Oracle Critical Patch Update - January 2015	CONFIRM	w
Security Advisory SA62480 - Oracle GlassFish Server Admin Console Vulnerability - Secunia	SECUNIA	se
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

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](#).

Free CVE JSON API [cve.report/api](#)

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