



CVE-2016-0441

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

Summary

CVE	CVE-2016-0441
State	PUBLISHED
Assigner	oracle
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-21 02:59:50 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Unspecified vulnerability in the Oracle GlassFish Server component in Oracle Fusion Middleware 3.1.2 allows remote auth

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

AV:N/AC:H/Au:S/C:C/I:C/A:P

Problem Types: NVD-CWE-noinfo | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Partial

AV:N/AC:H/Au:S/C:C/I:C/A:P

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference				
Sun GlassFish Enterprise Server Flaws Let Remote Authenticated Users Access and Modify Data and Partially Deny Service and Local Users				
Oracle Critical Patch Update - January 2016				
CVE Program record				
NVD vulnerability detail				
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				