



CVE-2007-2702

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

Summary

CVE	CVE-2007-2702
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-05-16 01:19:00 UTC
Updated	2018-10-30 16:25:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the GroupSpace application in BEA WebLogic Portal 9.2 GA allows remote auther

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Weblogic Portal	9.2	ga	All	All
Application	Oracle	Weblogic Portal	9.2	ga	All	All

References

Reference

- WebLogic Portal Input Validation Hole Permits Cross-Site Scripting Attacks and Entitlement Bug Lets Remote Users Access Resources - Secunia
- Cross-site scripting attacks in the WebLogic Portal Groupspace application
- Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
- 36066
- BEA Products Multiple Vulnerabilities - Advisories - Secunia
- IBM X-Force Exchange
- 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.

© [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](#)