



CVE-2007-5798

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

Summary

CVE	CVE-2007-5798
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-11-03 00:46:00 UTC
Updated	2017-07-29 01:33:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in uddigui/navigateTree.do in the UDDI user console in IBM WebSphere A

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Websphere Application Server	All	All	All	All

References

Reference

IBM WebSphere Application Server Input Validation Hole in 'uddigui/navigateTree.do' Page Permits Cross-Site Scripting Attacks - SecurityTra
41618
IBM WebSphere "uddigui/navigateTree.do" Cross-Site Scripting and Request Forgery - Advisories - Secunia
IBM WebSphere Application Server UDDI Console Multiple Input Validation Vulnerabilities
IBM X-Force Exchange
IBM PK50245: VALIDATION NEEDED FOR PARAMETERS THAT ARE PASSED TO THE NAVIGATETREE.DO PAGE IN THE UDDI USER
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
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](#).

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

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