



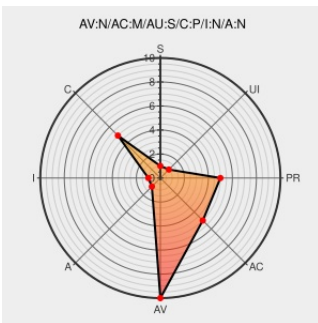
Last Modified on: 03/23/2021 11:23:16 PM UTC

CVE-2011-1503

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Liferay Portal](#) from [Liferay](#) contain the following vulnerability:

The XSL Content portlet in Liferay Portal Community Edition (CE) 5.x and 6.x before 6.0.6 GA, when Apache Tomcat or Oracle GlassFish is used, allows remote authenticated users to read arbitrary (1) XSL and (2) XML files via a file:/// URL.

CVE-2011-1503 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
oss-security - Re: CVE requests : Liferay 6.0.6	Mailing List Third Party Advisory openwall.com text/html	 MLIST [oss-security] 20110408 Re: CVE requests : Liferay 6.0.6
Liferay Issues - New Generation Issue Tracking	Issue Tracking Release Notes Vendor Advisory issues.liferay.com text/html	 CONFIRM issues.liferay.com/secure/ReleaseNote.jspa?version=10656&styleName=Html&projectId=10952
oss-security - CVE requests : Liferay 6.0.6	Mailing List Third Party Advisory openwall.com text/html	 MLIST [oss-security] 20110329 CVE requests : Liferay 6.0.6
[#] PS-13762 XSL Content Portlet can utilize file:/// to	Issue Tracking	 CONFIRM issues.liferay.com/browse/L PS-13762

CVET-2019-0217 CVE content format can allow users to potentially access files on the system - Liferay Issues

[Issue Tracking](#)[Vendor Advisory](#)[issues.liferay.com](#)[text/html](#)

[CVET-2019-0217 CVE content format can allow users to potentially access files on the system - Liferay Issues](#)

oss-security - Re: CVE requests : Liferay 6.0.6

[Mailing List](#)[Third Party Advisory](#)[openwall.com](#)[text/html](#)

 [MLIST \[oss-security\] 20110411 Re: CVE requests : Liferay 6.0.6](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Liferay	Liferay Portal	All	All	All	All
Application	Liferay	Liferay Portal	All	All	All	All
Application	Liferay	Liferay Portal	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows 7	-	All	All	All
Operating System	Microsoft	Windows 7	-	All	All	All
cpe:2.3:a:liferay:liferay_portal:*:*:*:community:*:*:						
cpe:2.3:a:liferay:liferay_portal:*:*:*:community:*:*:						
cpe:2.3:a:liferay:liferay_portal:*:*:*:community:*:*:						
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_7:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_7:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

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](#)