



# CVE-2015-4352

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

## Summary

<b>CVE</b>	CVE-2015-4352
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-06-15 14:59:00 UTC
<b>Updated</b>	2016-06-09 21:31:00 UTC
<b>Description</b>	Cross-site request forgery (CSRF) vulnerability in the Spider Video Player module for Drupal allows remote attackers to hijack

## Risk And Classification

**Problem Types:** CWE-352

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Web-dorado</a>	<a href="#">Web-dorado Spider Video Player</a>	-	All	All	All
Application	<a href="#">Web-dorado</a>	<a href="#">Web-dorado Spider Video Player</a>	-	All	All	All

## References

Reference	Source	Link
oss-security - CVE requests for Drupal contributed modules (from SA-CONTRIB-2015-034 to SA-CONTRIB-2015-099)	MLIST	<a href="#">www.oss-security.com</a>
Spider Video Player Module Arbitrary File Deletion and Cross Site Request Forgery Vulnerabilities	BID	<a href="#">www.securityfocus.com</a>
SA-CONTRIB-2015-059 - Spider Video Player - Multiple vulnerabilities - Unsupported   Drupal.org	MISC	<a href="#">www.drupal.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)**