



# CVE-2015-2087

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

## Summary

<b>CVE</b>	CVE-2015-2087
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-02-26 15:59:00 UTC
<b>Updated</b>	2015-02-27 17:43:00 UTC
<b>Description</b>	Unrestricted file upload vulnerability in the Avatar Uploader module before 6.x-1.3 for Drupal allows remote authenticated users to upload arbitrary files to the server.

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Avatar Uploader Project	Avatar Uploader	All	All	All	All

## References

Reference	Source	Link	Tags
avatar_uploader 6.x-1.3   Drupal.org	CONFIRM	<a href="http://www.drupal.org">www.drupal.org</a>	Patch
Drupal Avatar Uploader Module Arbitrary File Upload Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
SA-CONTRIB-2015-048 - Avatar Uploader - Arbitrary PHP code execution   Drupal.org	MISC	<a href="http://www.drupal.org">www.drupal.org</a>	Patch, Vendor
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, ar

No vendor comments have been submitted for this CVE.

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)