



CVE-2018-9205

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

Summary

CVE	CVE-2018-9205
State	PUBLIC
Assigner	larry0@me.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-04 15:29:00 UTC
Updated	2018-05-21 12:37:00 UTC
Description	Vulnerability in avatar_uploader v7.x-1.0-beta8 , The code in view.php doesn't verify users or sanitize the file path.

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Drupal	Avatar Uploader	7.x-1.0	beta8	All	All
Application	Drupal	Avatar Uploader	7.x-1.0	beta8	All	All

References

Reference	Source	Link
Vulnerability	MISC	www.vapidlab
Avatar Uploader Drupal.org	MISC	www.drupal.o
Drupal avatar_uploader v7.x-1.0-beta8 - Arbitrary File Disclosure - PHP webapps Exploit	EXPLOIT-DB	www.exploit-d
Arbitrary file download vulnerability in Drupal module avatar_uploader v7.x-1.0-beta8 [#2957966] Drupal.org	MISC	www.drupal.o
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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