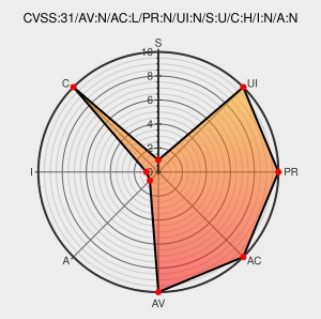
CVE-2011-2726

Published on: 11/15/2019 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:22 AM UTC

CVE-2011-2726

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

An access bypass issue was found in Drupal 7.x before version 7.5. If a Drupal site has the ability to attach File upload fields to any entity type in the system or has the ability to point individual File upload fields to the private file directory in comments, and the parent node is denied access, non-privileged users can still download the file attached to the comment if they know or guess its direct URL.

CVE-2011-2726 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **drupal core** - **drupal core** version **= 7.x before version 7.5**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link

Red Hat Customer Portal	Broken Link access.redhat.com text/html	MISC access.redhat.com/security/cve/cve-2011-2726
SA-CORE-2011-003 - Drupal core - Access bypass | drupal.org	Vendor Advisory www.drupal.org text/html	CONFIRM www.drupal.org/node/1231510
Bug 726222 – drupal7: access bypass vulnerability in 7.x (SA-CORE-2011-003)	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-2726
oss-security - Re: Re: [security] Drupal CORE and Drupal Contrib	Mailing List Third Party Advisory www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2012/03/19/10
CVE-2011-2726	Third Party Advisory security-tracker.debian.org text/html	MISC security-tracker.debian.org/tracker/CVE-2011-2726
oss-security - Re: Re: [security] Drupal CORE and Drupal Contrib	Mailing List Third Party Advisory www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2012/03/20/14

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Drupal	Drupal	All	All	All	All
Application	Drupal	Drupal	All	All	All	All
Operating System	Fedoraproject	Fedora	14	All	All	All
Operating System	Fedoraproject	Fedora	15	All	All	All
Operating System	Fedoraproject	Fedora	16	All	All	All
Operating	Fedoraproject	Fedora	14	All	All	All

System						
Operating System	Fedoraproject	Fedora	15	All	All	All
Operating System	Fedoraproject	Fedora	16	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All

- cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:
- cpe:2.3:a:drupal:drupal:*:*:*:*:*:*:*:*:
- cpe:2.3:a:drupal:drupal:*:*:*:*:*:*:*:*:
- cpe:2.3:o:fedoraproject:fedora:14:*:*:*:*:*:*:*:
- cpe:2.3:o:fedoraproject:fedora:15:*:*:*:*:*:*:*:
- cpe:2.3:o:fedoraproject:fedora:16:*:*:*:*:*:*:*:
- cpe:2.3:o:fedoraproject:fedora:14:*:*:*:*:*:*:*:
- cpe:2.3:o:fedoraproject:fedora:15:*:*:*:*:*:*:*:
- cpe:2.3:o:fedoraproject:fedora:16:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux:5.0:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux:5.0:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report