

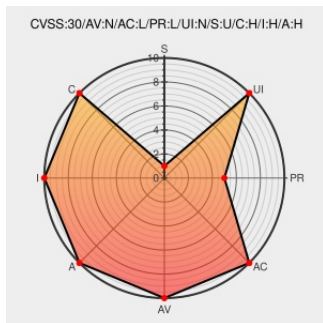


CVE-2016-6211

Published on: 09/09/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:11 PM UTC

CVE-2016-6211

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

The User module in Drupal 7.x before 7.44 allows remote authenticated users to gain privileges via vectors involving contributed or custom code that triggers a rebuild of the user profile form.

CVE-2016-6211 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-3604-1 drupal7	Third Party Advisory www.debian.org Deprecated Link text/html	DEBIAN DSA-3604

Drupal DRUPAL-SA-CORE-2016-002 Privilege Escalation and Access Bypass Vulnerabilities	cve.report (archive) text/html	 BID 91230
oss-security - Re: CVE requests for Drupal Core - SA-CORE-2016-002	Mailing List Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20160713 Re: CVE requests for Drupal Core - SA-CORE-2016-002
oss-security - CVE requests for Drupal Core - SA-CORE-2016-002	Mailing List Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20160713 CVE requests for Drupal Core - SA-CORE-2016-002
Drupal Core - Moderately Critical - Multiple Vulnerabilities - SA-CORE-2016-002 Drupal.org	Vendor Advisory www.drupal.org text/html	 CONFIRM www.drupal.org/SA-CORE-2016-002

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
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Drupal	Drupal	7.0	All	All	All
Application	Drupal	Drupal	7.0	alpha1	All	All
Application	Drupal	Drupal	7.0	alpha2	All	All
Application	Drupal	Drupal	7.0	alpha3	All	All
Application	Drupal	Drupal	7.0	alpha4	All	All
Application	Drupal	Drupal	7.0	alpha5	All	All
Application	Drupal	Drupal	7.0	alpha6	All	All
Application	Drupal	Drupal	7.0	alpha7	All	All
Application	Drupal	Drupal	7.0	beta1	All	All
Application	Drupal	Drupal	7.0	beta2	All	All
Application	Drupal	Drupal	7.0	beta3	All	All
Application	Drupal	Drupal	7.0	dev	All	All
Application	Drupal	Drupal	7.0	rc1	All	All
Application	Drupal	Drupal	7.0	rc2	All	All
Application	Drupal	Drupal	7.0	rc3	All	All
Application	Drupal	Drupal	7.0	rc4	All	All

Application	Drupal	Drupal	7.1	All	All	All
Application	Drupal	Drupal	7.10	All	All	All
Application	Drupal	Drupal	7.11	All	All	All
Application	Drupal	Drupal	7.12	All	All	All
Application	Drupal	Drupal	7.13	All	All	All
Application	Drupal	Drupal	7.14	All	All	All
Application	Drupal	Drupal	7.15	All	All	All
Application	Drupal	Drupal	7.16	All	All	All
Application	Drupal	Drupal	7.17	All	All	All
Application	Drupal	Drupal	7.18	All	All	All
Application	Drupal	Drupal	7.19	All	All	All
Application	Drupal	Drupal	7.2	All	All	All
Application	Drupal	Drupal	7.20	All	All	All
Application	Drupal	Drupal	7.21	All	All	All
Application	Drupal	Drupal	7.22	All	All	All
Application	Drupal	Drupal	7.23	All	All	All
Application	Drupal	Drupal	7.24	All	All	All
Application	Drupal	Drupal	7.25	All	All	All
Application	Drupal	Drupal	7.26	All	All	All
Application	Drupal	Drupal	7.27	All	All	All
Application	Drupal	Drupal	7.28	All	All	All
Application	Drupal	Drupal	7.29	All	All	All
Application	Drupal	Drupal	7.3	All	All	All
Application	Drupal	Drupal	7.30	All	All	All
Application	Drupal	Drupal	7.31	All	All	All
Application	Drupal	Drupal	7.32	All	All	All
Application	Drupal	Drupal	7.33	All	All	All
Application	Drupal	Drupal	7.34	All	All	All
Application	Drupal	Drupal	7.35	All	All	All
Application	Drupal	Drupal	7.36	All	All	All
Application	Drupal	Drupal	7.37	All	All	All
Application	Drupal	Drupal	7.38	All	All	All
Application	Drupal	Drupal	7.39	All	All	All
Application	Drupal	Drupal	7.4	All	All	All
Application	Drupal	Drupal	7.40	All	All	All

Application	Drupal	Drupal	7.41	All	All	All
Application	Drupal	Drupal	7.42	All	All	All
Application	Drupal	Drupal	7.43	All	All	All
Application	Drupal	Drupal	7.5	All	All	All
Application	Drupal	Drupal	7.6	All	All	All
Application	Drupal	Drupal	7.7	All	All	All
Application	Drupal	Drupal	7.8	All	All	All
Application	Drupal	Drupal	7.9	All	All	All
Application	Drupal	Drupal	7.x-dev	All	All	All
Application	Drupal	Drupal	7.0	All	All	All
Application	Drupal	Drupal	7.0	alpha1	All	All
Application	Drupal	Drupal	7.0	alpha2	All	All
Application	Drupal	Drupal	7.0	alpha3	All	All
Application	Drupal	Drupal	7.0	alpha4	All	All
Application	Drupal	Drupal	7.0	alpha5	All	All
Application	Drupal	Drupal	7.0	alpha6	All	All
Application	Drupal	Drupal	7.0	alpha7	All	All
Application	Drupal	Drupal	7.0	beta1	All	All
Application	Drupal	Drupal	7.0	beta2	All	All
Application	Drupal	Drupal	7.0	beta3	All	All
Application	Drupal	Drupal	7.0	dev	All	All
Application	Drupal	Drupal	7.0	rc1	All	All
Application	Drupal	Drupal	7.0	rc2	All	All
Application	Drupal	Drupal	7.0	rc3	All	All
Application	Drupal	Drupal	7.0	rc4	All	All
Application	Drupal	Drupal	7.1	All	All	All
Application	Drupal	Drupal	7.10	All	All	All
Application	Drupal	Drupal	7.11	All	All	All
Application	Drupal	Drupal	7.12	All	All	All
Application	Drupal	Drupal	7.13	All	All	All
Application	Drupal	Drupal	7.14	All	All	All
Application	Drupal	Drupal	7.15	All	All	All
Application	Drupal	Drupal	7.16	All	All	All
Application	Drupal	Drupal	7.17	All	All	All
Application	Drupal	Drupal	7.18	All	All	All
Application	Drupal	Drupal	7.19	All	All	All


```

cpe:2.3.0:debian:debian_i386:0.0. . . . .

```

cpe:2.3:a:drupal:drupal:7.0:*:*:*:*:*:*:

```
cpe:2.3:a:drupal:drupal:7.0:alpha1:::*:*:*:
```

```
cpe:2.3:a:drupal:drupal:7.0:alpha2:*:*:*:*:*:*
```

```
cpe:2.3:a:drupal:drupal:7.0:alpha3:*:*:*:*:*:
```

```
cpe:2.3:a:drupal:drupal:7.0:alpha4:*:*:*:*:*:
```

```
cpe:2.3:a:drupal:drupal:7.0:alpha5:*:*:*:*:*:
```

```
cpe:2.3:a:drupal:drupal:7.0:alpha6:*:*:*:*:*:
```

cpe:2.3:a:drupal:drupal:7.0:alpha7:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.0:beta1:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.0:beta2:*:*:*:*:*:

```
cpe:2.3:a:drupal:drupal:7.0:beta3:*:*:*:*:*:
```

```
cpe:2.3:a:drupal:drupal:7.0:dev:*:*:*:*:*:
```

cpe:2.3:a:drupal:drupal:7.0:rc1:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.0:rc2:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.0:rc3:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.0:rc4:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.1:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.10:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.11:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.12:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.13:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.14:*:*:*:*:*:*

cpe:2.3:a:drupal:drupal:7.15:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.16:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.17:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.18:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.19:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.2:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.20:*****:*
cpe:2.3:a:drupal:drupal:7.21:*****:*
cpe:2.3:a:drupal:drupal:7.22:*****:*
cpe:2.3:a:drupal:drupal:7.23:*****:*
cpe:2.3:a:drupal:drupal:7.24:*****:*
cpe:2.3:a:drupal:drupal:7.25:*****:*
cpe:2.3:a:drupal:drupal:7.26:*****:*
cpe:2.3:a:drupal:drupal:7.27:*****:*
cpe:2.3:a:drupal:drupal:7.28:*****:*
cpe:2.3:a:drupal:drupal:7.29:*****:*
cpe:2.3:a:drupal:drupal:7.3:*****:*
cpe:2.3:a:drupal:drupal:7.30:*****:*
cpe:2.3:a:drupal:drupal:7.31:*****:*
cpe:2.3:a:drupal:drupal:7.32:*****:*
cpe:2.3:a:drupal:drupal:7.33:*****:*
cpe:2.3:a:drupal:drupal:7.34:*****:*
cpe:2.3:a:drupal:drupal:7.35:*****:*
cpe:2.3:a:drupal:drupal:7.36:*****:*
cpe:2.3:a:drupal:drupal:7.37:*****:*
cpe:2.3:a:drupal:drupal:7.38:*****:*
cpe:2.3:a:drupal:drupal:7.39:*****:*
cpe:2.3:a:drupal:drupal:7.4:*****:*
cpe:2.3:a:drupal:drupal:7.40:*****:*
cpe:2.3:a:drupal:drupal:7.41:*****:*
cpe:2.3:a:drupal:drupal:7.42:*****:*
cpe:2.3:a:drupal:drupal:7.43:*****:*
cpe:2.3:a:drupal:drupal:7.5:*****:*
cpe:2.3:a:drupal:drupal:7.6:*****:*

cpe:2.3:a:drupal:drupal:7.7:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.8:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.9:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.x-dev:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.0:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.0:alpha1:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.0:alpha2:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.0:alpha3:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.0:alpha4:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.0:alpha5:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.0:alpha6:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.0:alpha7:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.0:beta1:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.0:beta2:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.0:beta3:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.0:dev:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.0:rc1:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.0:rc2:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.0:rc3:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.0:rc4:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.1:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.10:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.11:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.12:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.13:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.14:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.15:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.16:*:*:*:*:*:
cpe:2.3:a:drupal:drupal:7.17:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.18:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.19:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.2:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.20:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.21:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.22:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.23:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.24:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.25:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.26:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.27:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.28:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.29:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.3:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.30:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.31:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.32:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.33:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.34:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.35:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.36:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.37:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.38:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.39:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.4:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.40:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.41:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.42:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:7.43:*****:
cpe:2.3:a:drupal:drupal:7.5:*****:
cpe:2.3:a:drupal:drupal:7.6:*****:
cpe:2.3:a:drupal:drupal:7.7:*****:
cpe:2.3:a:drupal:drupal:7.8:*****:
cpe:2.3:a:drupal:drupal:7.9:*****:
cpe:2.3:a:drupal:drupal:7.x-dev:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [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](#)