



CVE-2014-3704

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

Summary

CVE	CVE-2014-3704
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-16 00:55:00 UTC
Updated	2021-09-29 14:08:00 UTC
Description	The expandArguments function in the database abstraction API in Drupal core 7.x before 7.32 does not properly construct p

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Drupal	Drupal	All	All	All	All
Application	Drupal	Drupal Core	7.0	All	All	All
Application	Drupal	Drupal Core	7.01	All	All	All
Application	Drupal	Drupal Core	7.02	All	All	All
Application	Drupal	Drupal Core	7.03	All	All	All
Application	Drupal	Drupal Core	7.04	All	All	All
Application	Drupal	Drupal Core	7.05	All	All	All
Application	Drupal	Drupal Core	7.06	All	All	All
Application	Drupal	Drupal Core	7.07	All	All	All
Application	Drupal	Drupal Core	7.08	All	All	All
Application	Drupal	Drupal Core	7.09	All	All	All
Application	Drupal	Drupal Core	7.10	All	All	All
Application	Drupal	Drupal Core	7.11	All	All	All
Application	Drupal	Drupal Core	7.12	All	All	All
Application	Drupal	Drupal Core	7.13	All	All	All
Application	Drupal	Drupal Core	7.14	All	All	All

Application	Drupal	Drupal Core	7.15	All	All	All
Application	Drupal	Drupal Core	7.16	All	All	All
Application	Drupal	Drupal Core	7.17	All	All	All
Application	Drupal	Drupal Core	7.18	All	All	All
Application	Drupal	Drupal Core	7.19	All	All	All
Application	Drupal	Drupal Core	7.20	All	All	All
Application	Drupal	Drupal Core	7.21	All	All	All
Application	Drupal	Drupal Core	7.22	All	All	All
Application	Drupal	Drupal Core	7.23	All	All	All
Application	Drupal	Drupal Core	7.24	All	All	All
Application	Drupal	Drupal Core	7.25	All	All	All
Application	Drupal	Drupal Core	7.26	All	All	All
Application	Drupal	Drupal Core	7.27	All	All	All
Application	Drupal	Drupal Core	7.28	All	All	All
Application	Drupal	Drupal Core	7.29	All	All	All
Application	Drupal	Drupal Core	7.30	All	All	All
Application	Drupal	Drupal Core	7.31	All	All	All
Application	Drupal	Drupal Core	7.0	All	All	All
Application	Drupal	Drupal Core	7.01	All	All	All
Application	Drupal	Drupal Core	7.02	All	All	All
Application	Drupal	Drupal Core	7.03	All	All	All
Application	Drupal	Drupal Core	7.04	All	All	All
Application	Drupal	Drupal Core	7.05	All	All	All
Application	Drupal	Drupal Core	7.06	All	All	All
Application	Drupal	Drupal Core	7.07	All	All	All
Application	Drupal	Drupal Core	7.08	All	All	All
Application	Drupal	Drupal Core	7.09	All	All	All
Application	Drupal	Drupal Core	7.10	All	All	All
Application	Drupal	Drupal Core	7.11	All	All	All
Application	Drupal	Drupal Core	7.12	All	All	All
Application	Drupal	Drupal Core	7.13	All	All	All
Application	Drupal	Drupal Core	7.14	All	All	All
Application	Drupal	Drupal Core	7.15	All	All	All
Application	Drupal	Drupal Core	7.16	All	All	All
Application	Drupal	Drupal Core	7.17	All	All	All

Application	Drupal	Drupal Core	7.18	All	All	All
Application	Drupal	Drupal Core	7.19	All	All	All
Application	Drupal	Drupal Core	7.20	All	All	All
Application	Drupal	Drupal Core	7.21	All	All	All
Application	Drupal	Drupal Core	7.22	All	All	All
Application	Drupal	Drupal Core	7.23	All	All	All
Application	Drupal	Drupal Core	7.24	All	All	All
Application	Drupal	Drupal Core	7.25	All	All	All
Application	Drupal	Drupal Core	7.26	All	All	All
Application	Drupal	Drupal Core	7.27	All	All	All
Application	Drupal	Drupal Core	7.28	All	All	All
Application	Drupal	Drupal Core	7.29	All	All	All
Application	Drupal	Drupal Core	7.30	All	All	All
Application	Drupal	Drupal Core	7.31	All	All	All

References

Reference	Source	Link	Tags
SA-CORE-2014-005 - Drupal core - SQL injection Drupal.org	CONFIRM	www.drupal.org	Patch, Ven
Drupal 7.X SQL Injection ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit
Drupal Core <= 7.32 - SQL Injection (#2)	EXPLOIT-DB	www.exploit-db.com	Exploit
Drupal HTTP Parameter Key/Value SQL Injection ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit
Drupal < 7.32 Pre Auth SQL Injection	EXPLOIT-DB	www.exploit-db.com	Exploit
Full Disclosure: Advisory 01/2014: Drupal7 - pre Auth SQL Injection Vulnerability	FULLDISC	seclists.org	
oss-security - Advisory 01/2014: Drupal7 - pre Auth SQL Injection Vulnerability	MLIST	www.openwall.com	Exploit
113371	OSVDB	osvdb.org	
Drupal Core CVE-2014-3704 SQL Injection Vulnerability	BID	www.securityfocus.com	
SecurityFocus	BUGTRAQ	www.securityfocus.com	
Drupal 7.31 SQL Injection ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit
Drupal 7.32 two weeks later - PoC SektionEins GmbH	MISC	www.sektioneins.de	
Drupal Core <= 7.32 - SQL Injection (PHP)	EXPLOIT-DB	www.exploit-db.com	Exploit
Debian -- Security Information -- DSA-3051-1 drupal7	DEBIAN	www.debian.org	
Drupal Core <= 7.32 - SQL Injection (#1)	EXPLOIT-DB	www.exploit-db.com	Exploit
Advisory 01/2014: Drupal - pre Auth SQL Injection Vulnerability SektionEins GmbH	MISC	www.sektioneins.de	Exploit
About Secunia Research Flexera	SECUNIA	secunia.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#)