



CVE-2015-7857

Published on: 10/29/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-7857

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

Certain versions of [Joomla!](#) from [Joomla](#) contain the following vulnerability:

SQL injection vulnerability in the getListQuery function in administrator/components/com_contenthistory/models/history.php in Joomla! 3.2 before 3.4.5 allows remote attackers to execute arbitrary SQL commands via the list[select] parameter to index.php.

CVE-2015-7857 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

[20151001] - Core - SQL Injection

[developer.joomla.org](#)
[text/html](#)

[CONFIRM developer.joomla.org/security-centre/628-20151001-core-sql-injection.html](#)

Joomla! 3.4.4 Component Content History - SQL Injection / Remote Code Execution (Metasploit) - PHP remote Exploit

[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

[EXPLOIT-DB 38797](#)

Joomla 3.44 SQL Injection ~ Packet Storm

[packetstormsecurity.com](#)
[text/html](#)

[MISC packetstormsecurity.com/files/134097/Joomla-3.44-SQL-Injection.html](#)

Joomla! Core Bugs Let Remote Users Bypass Access Controls and Inject SQL Commands - SecurityTracker

[www.securitytracker.com](#)
[text/html](#)

[SECTRACK 1033950](#)

Joomla SQL Injection Vulnerability Exploit Results in Full Administrative Access	Exploit www.trustwave.com text/html	 MISC www.trustwave.com/Resources/SpiderLabs-Blog/Joomla-SQL-Injection-Vulnerability-Exploit-Results-in-Full-Administrative-Access/
Joomla Content History SQL Injection Remote Code Execution ~ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/134494/Joomla-Content-History-SQL-Injection-Remote-Code-Execution.html
CVE-2015-7857 Joomla Content History SQLi Remote Code Execution Rapid7	www.rapid7.com text/html	 MISC www.rapid7.com/db/modules/exploit/unix/webapp/joomla_contenthistory_sql_i_rce
Joomla! Core Multiple SQL Injection Vulnerabilities	cve.report (archive) text/html	 BID 77295

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

Exploit/POC from Github

Joomla! 3.2 to 3.4.4 - SQL Injection (CVE-2015-7297, CVE-2015-7857, and CVE-2015-7858)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Joomla	Joomla!	3.2.0	All	All	All
Application	Joomla	Joomla!	3.2.1	All	All	All
Application	Joomla	Joomla!	3.2.2	All	All	All
Application	Joomla	Joomla!	3.2.3	All	All	All
Application	Joomla	Joomla!	3.2.4	All	All	All
Application	Joomla	Joomla!	3.3.0	All	All	All
Application	Joomla	Joomla!	3.3.1	All	All	All
Application	Joomla	Joomla!	3.3.2	All	All	All
Application	Joomla	Joomla!	3.3.3	All	All	All
Application	Joomla	Joomla!	3.3.4	All	All	All
Application	Joomla	Joomla!	3.4.0	All	All	All
Application	Joomla	Joomla!	3.4.1	All	All	All
Application	Joomla	Joomla!	3.4.2	All	All	All
Application	Joomla	Joomla!	3.4.3	All	All	All
Application	Joomla	Joomla!	3.4.4	All	All	All
Application	Joomla	Joomla!	3.2.0	All	All	All
Application	Joomla	Joomla!	3.2.1	All	All	All

Application	Joomla	Joomla!	3.2.2	All	All	All
Application	Joomla	Joomla!	3.2.3	All	All	All
Application	Joomla	Joomla!	3.2.4	All	All	All
Application	Joomla	Joomla!	3.3.0	All	All	All
Application	Joomla	Joomla!	3.3.1	All	All	All
Application	Joomla	Joomla!	3.3.2	All	All	All
Application	Joomla	Joomla!	3.3.3	All	All	All
Application	Joomla	Joomla!	3.3.4	All	All	All
Application	Joomla	Joomla!	3.4.0	All	All	All
Application	Joomla	Joomla!	3.4.1	All	All	All
Application	Joomla	Joomla!	3.4.2	All	All	All
Application	Joomla	Joomla!	3.4.3	All	All	All
Application	Joomla	Joomla!	3.4.4	All	All	All
Application	Joomla	Joomla!	3.2.0	All	All	All
Application	Joomla	Joomla!	3.2.1	All	All	All
Application	Joomla	Joomla!	3.2.2	All	All	All
Application	Joomla	Joomla!	3.2.3	All	All	All
Application	Joomla	Joomla!	3.2.4	All	All	All
Application	Joomla	Joomla!	3.3.0	All	All	All
Application	Joomla	Joomla!	3.3.1	All	All	All
Application	Joomla	Joomla!	3.3.2	All	All	All
Application	Joomla	Joomla!	3.3.3	All	All	All
Application	Joomla	Joomla!	3.3.4	All	All	All
Application	Joomla	Joomla!	3.4.0	All	All	All
Application	Joomla	Joomla!	3.4.1	All	All	All
Application	Joomla	Joomla!	3.4.2	All	All	All
Application	Joomla	Joomla!	3.4.3	All	All	All
Application	Joomla	Joomla!	3.4.4	All	All	All
cpe:2.3:a:joomla:joomla!:3.2.0:*****:						
cpe:2.3:a:joomla:joomla!:3.2.1:*****:						
cpe:2.3:a:joomla:joomla!:3.2.2:*****:						
cpe:2.3:a:joomla:joomla!:3.2.3:*****:						
cpe:2.3:a:joomla:joomla!:3.2.4:*****:						
cpe:2.3:a:joomla:joomla!:3.3.0:*****:						

cpe:2.3:a:joomla:joomla!:3.3.1:*****:
cpe:2.3:a:joomla:joomla!:3.3.2:*****:
cpe:2.3:a:joomla:joomla!:3.3.3:*****:
cpe:2.3:a:joomla:joomla!:3.3.4:*****:
cpe:2.3:a:joomla:joomla!:3.4.0:*****:
cpe:2.3:a:joomla:joomla!:3.4.1:*****:
cpe:2.3:a:joomla:joomla!:3.4.2:*****:
cpe:2.3:a:joomla:joomla!:3.4.3:*****:
cpe:2.3:a:joomla:joomla!:3.4.4:*****:
cpe:2.3:a:joomla:joomla\!:3.2.0:*****:
cpe:2.3:a:joomla:joomla\!:3.2.1:*****:
cpe:2.3:a:joomla:joomla\!:3.2.2:*****:
cpe:2.3:a:joomla:joomla\!:3.2.3:*****:
cpe:2.3:a:joomla:joomla\!:3.2.4:*****:
cpe:2.3:a:joomla:joomla\!:3.3.0:*****:
cpe:2.3:a:joomla:joomla\!:3.3.1:*****:
cpe:2.3:a:joomla:joomla\!:3.3.2:*****:
cpe:2.3:a:joomla:joomla\!:3.3.3:*****:
cpe:2.3:a:joomla:joomla\!:3.3.4:*****:
cpe:2.3:a:joomla:joomla\!:3.4.0:*****:
cpe:2.3:a:joomla:joomla\!:3.4.1:*****:
cpe:2.3:a:joomla:joomla\!:3.4.2:*****:
cpe:2.3:a:joomla:joomla\!:3.4.3:*****:
cpe:2.3:a:joomla:joomla\!:3.4.4:*****:
cpe:2.3:a:joomla:joomla\!:3.2.0:*****:
cpe:2.3:a:joomla:joomla\!:3.2.1:*****:
cpe:2.3:a:joomla:joomla\!:3.2.2:*****:
cpe:2.3:a:joomla:joomla\!:3.2.3:*****:

cpe:2.3:a:joomla:joomla\!:3.2.4.*:*:*:*:*:
cpe:2.3:a:joomla:joomla\!:3.3.0.*:*:*:*:*:
cpe:2.3:a:joomla:joomla\!:3.3.1.*:*:*:*:*:
cpe:2.3:a:joomla:joomla\!:3.3.2.*:*:*:*:*:
cpe:2.3:a:joomla:joomla\!:3.3.3.*:*:*:*:*:
cpe:2.3:a:joomla:joomla\!:3.3.4.*:*:*:*:*:
cpe:2.3:a:joomla:joomla\!:3.4.0.*:*:*:*:*:
cpe:2.3:a:joomla:joomla\!:3.4.1.*:*:*:*:*:
cpe:2.3:a:joomla:joomla\!:3.4.2.*:*:*:*:*:
cpe:2.3:a:joomla:joomla\!:3.4.3.*:*:*:*:*:
cpe:2.3:a:joomla:joomla\!:3.4.4.*:*:*:*:*:

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