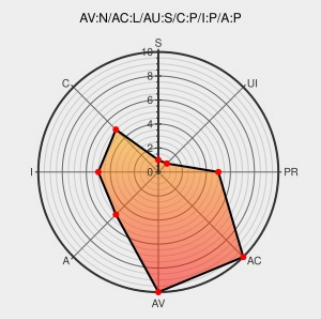
CVE-2015-1397

Published on: 04/29/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:10 PM UTC

CVE-2015-1397

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



Certain versions of Magento from Magento contain the following vulnerability:

SQL injection vulnerability in the getCsvFile function in the Mage_Adminhtml_Block_Widget_Grid class in Magento Community Edition (CE) 1.9.1.0 and Enterprise Edition (EE) 1.14.1.0 allows remote administrators to execute arbitrary SQL commands via the popularity[field_expr] parameter when the popularity[from] or popularity[to] parameter is set.

CVE-2015-1397 has been assigned by cve@mitre.org to track the vulnerability

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
Critical Security Advisory: Remote Code Execution (RCE) Vulnerability | Magento	Vendor Advisory, magento.com, text/html	CONFIRM magento.com/blog/technical/critical-security-advisory-remote-code-execution-rce-vulnerability
Analyzing the Magento Vulnerability (Updated) | Check Point Blog	blog.checkpoint.com, text/html	MISC blog.checkpoint.com/2015/04/20/analyzing-magento-vulnerability/
Magento Bugs Let Remote Users Execute Arbitrary PHP Code - SecurityTracker	www.securitytracker.com, text/html	SECTRACK 1032194
Magento Shoplift (SUPEE-5344) Exploits in the Wild - Sucuri Blog	Exploit, blog.sucuri.net, text/html	MISC blog.sucuri.net/2015/04/magento-shoplift-supee-5344-exploits-in-the-wild.html

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
Application	Magento	Magento	1.14.1.0	All	All	All
Application	Magento	Magento	1.9.1.0	All	All	All
Application	Magento	Magento	1.14.1.0	All	All	All
Application	Magento	Magento	1.9.1.0	All	All	All

cpe:2.3:a:magento:magento:1.14.1.0:*:*:*:enterprise:*:*:*:

cpe:2.3:a:magento:magento:1.9.1.0:*:*:*:community:*:*:*:

cpe:2.3:a:magento:magento:1.14.1.0:*:*:*:enterprise:*:*:*:

cpe:2.3:a:magento:magento:1.9.1.0:*:*:*:community:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→