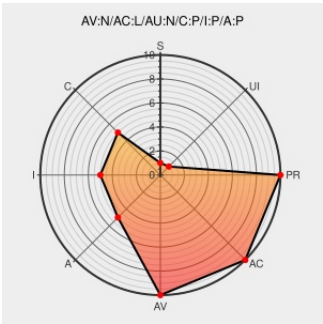
CVE-2014-9115

Published on: 12/23/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:00 PM UTC

CVE-2014-9115

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



Certain versions of Piwigo from Piwigo contain the following vulnerability:

SQL injection vulnerability in the rate_picture function in include/functions_rate.inc.php in Piwigo before 2.5.5, 2.6.x before 2.6.4, and 2.7.x before 2.7.2 allows remote attackers to execute arbitrary SQL commands via the rate parameter to picture.php, related to an improper data type in a comparison of a non-numeric value that begins with a digit.

CVE-2014-9115 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Full Disclosure: Piwigo <= v2.6.0 - Blind SQL Injection	Exploit, seclists.org, text/html	FULLDISC 20141112 Piwigo <= v2.6.0 - Blind SQL Injection
Changeset 30563 for trunk/include/functions_rate.inc.php – piwigo	piwigo.org, text/html	CONFIRM piwigo.org/dev/changeset/30563/trunk/include/functions_rate.inc.php
Piwigo 2.7.2, 2.6.4, 2.5.5, Security Bug Fixed | Piwigo.org	Vendor Advisory, piwigo.org, text/html	CONFIRM piwigo.org/forum/viewtopic.php?id=24850
Piwigo 2.7.2 Release Notes | piwigo.org	Patch, web.archive.org	CONFIRM piwigo.org/releases/2.7.2

text/html

Inactive Link | Not Archived

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	Piwigo	Piwigo	2.6.0	All	All	All
Application	Piwigo	Piwigo	2.6.1	All	All	All
Application	Piwigo	Piwigo	2.6.2	All	All	All
Application	Piwigo	Piwigo	2.6.3	All	All	All
Application	Piwigo	Piwigo	2.7.0	All	All	All
Application	Piwigo	Piwigo	2.7.0	beta1	All	All
Application	Piwigo	Piwigo	2.7.0	beta2	All	All
Application	Piwigo	Piwigo	2.7.0	rc1	All	All
Application	Piwigo	Piwigo	2.7.0	rc2	All	All
Application	Piwigo	Piwigo	2.7.1	All	All	All
Application	Piwigo	Piwigo	2.6.0	All	All	All
Application	Piwigo	Piwigo	2.6.1	All	All	All
Application	Piwigo	Piwigo	2.6.2	All	All	All
Application	Piwigo	Piwigo	2.6.3	All	All	All
Application	Piwigo	Piwigo	2.7.0	All	All	All
Application	Piwigo	Piwigo	2.7.0	beta1	All	All
Application	Piwigo	Piwigo	2.7.0	beta2	All	All
Application	Piwigo	Piwigo	2.7.0	rc1	All	All
Application	Piwigo	Piwigo	2.7.0	rc2	All	All
Application	Piwigo	Piwigo	2.7.1	All	All	All
Application	Piwigo	Piwigo	All	All	All	All

cpe:2.3:a:piwigo:piwigo:2.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.6.3:*:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.7.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.7.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.7.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.7.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.7.1:*:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.6.3:*:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.7.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.7.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.7.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.7.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.7.1:*:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→