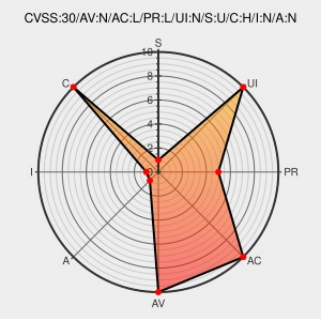
CVE-2017-9463

Published on: 06/14/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:56 PM UTC

CVE-2017-9463

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



Certain versions of Piwigo from Piwigo contain the following vulnerability:

The application Piwigo is affected by a SQL injection vulnerability in version 2.9.0 and possibly prior. This vulnerability allows remote authenticated attackers to obtain information in the context of the user used by the application to retrieve data from the database. The user_list_backend.php component is affected: values of the iDisplayStart & iDisplayLength parameters are not sanitized; these are used to construct a SQL query and retrieve a list of registered users into the application.

CVE-2017-9463 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
wizlynx group | SQL Injection		MISC www.wizlynxgroup.com/security-research-advisories/vuln/WLX-2017-002

wizlynx group | SQL Injection in Piwigo	Issue Tracking Third Party Advisory www.wizlynxgroup.com text/html	MISC www.wizlynxgroup.com/security-research-advisories/vuln/WLX-2017-003
user list backend, check input parameter · Issue #705 · Piwigo/Piwigo · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/Piwigo/Piwigo/issues/705
(cp 6ce14fc) fixes #705, check user_list_backend.php input params · Piwigo/Piwigo@4292089 · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/Piwigo/Piwigo/commit/42920897ce927c236728d387f61bf03d117109a2

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	All	All	All	All

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→