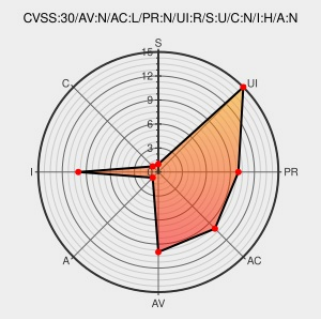
CVE-2016-10514

Published on: 10/10/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:00 PM UTC

CVE-2016-10514

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



Certain versions of Piwigo from Piwigo contain the following vulnerability:

url_check_format in include/functions.inc.php in Piwigo before 2.8.3 allows remote attackers to bypass intended access restrictions via a URL that contains a " character, or a URL beginning with a substring other than the http:// or https:// substring.

CVE-2016-10514 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	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
fixes #547, strong checks on url format · Piwigo/Piwigo@b3157cb · GitHub	Issue Tracking, Patch, Third Party Advisory, github.com, text/html	CONFIRM github.com/Piwigo/Piwigo/commit/b3157cbfd859c914911b114d4edbba4654758b57

Piwigo 2.8.3 Release Notes | piwigo.org	Patch Release Notes Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM piwigo.org/releases/2.8.3
increase checks on url format · Issue #547 · Piwigo/Piwigo · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	CONFIRM github.com/Piwigo/Piwigo/issues/547

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→