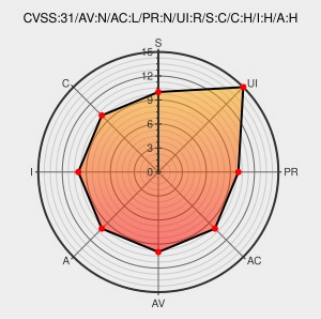
CVE-2019-13364

Published on: 09/13/2019 12:00:00 AM UTC

Last Modified on: 02/28/2023 03:27:00 PM UTC

CVE-2019-13364

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



Certain versions of Piwigo from Piwigo contain the following vulnerability:

admin.php?page=account_billing in Piwigo 2.9.5 has XSS via the vat_number, billing_name, company, or billing_address parameter. This is exploitable via CSRF.

CVE-2019-13364 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.6 - CRITICAL

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Full Disclosure: Piwigo - Version 2.9.5 [CVE-2019-13363, CVE-2019-13364]	Mailing List Third Party Advisory seclists.org text/html	MISC seclists.org/fulldisclosure/2019/Sep/25

Issues · Piwigo/Piwigo · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/Piwigo/Piwigo/issues
Piwigo - Image library software and Digital Asset Management	Vendor Advisory piwigo.com text/html	MISC piwigo.com
Piwigo 2.9.5 Cross Site Request Forgery / Cross Site Scripting ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/154484/Piwigo-2.9.5-Cross-Site-Request-Forgery-Cross-Site-Scripting.html
Full Disclosure: GilaCMS - CVE-2019-13364 CVE-2019-13363	seclists.org text/html	FULLDISC 20200623 GilaCMS - CVE-2019-13364 CVE-2019-13363

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	2.9.5	All	All	All
Application	Piwigo	Piwigo	2.9.5	All	All	All

cpe:2.3:a:piwigo:piwigo:2.9.5:*:*:*:*:*:*:*:

cpe:2.3:a:piwigo:piwigo:2.9.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→