



CVE-2019-13363

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

Last Modified on: 02/28/2023 03:26:00 PM UTC

CVE-2019-13363

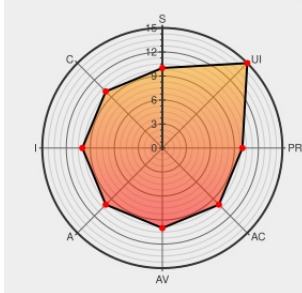
Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

CVSS:31/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H



Certain versions of [Piwigo](#) from [Piwigo](#) contain the following vulnerability:

admin.php?page=notification_by_mail in Piwigo 2.9.5 has XSS via the nbm_send_html_mail, nbm_send_mail_as, nbm_send_detailed_content, nbm_complementary_mail_content, nbm_send_recent_post_dates, or param_submit parameter. This is exploitable via CSRF.

CVE-2019-13363 has been assigned by [M](#) 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	MISC seclists.org/fulldisclosure/2019/Sep/25

seclists.org
text/html

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

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	2.9.5	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→		