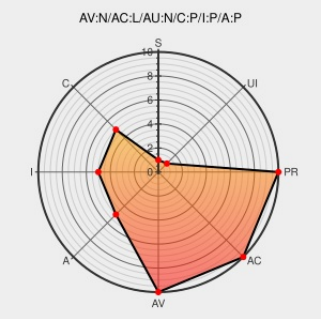
CVE-2003-1227

Published on: 12/31/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:43 PM UTC

CVE-2003-1227

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



Certain versions of Gallery from Gallery Project contain the following vulnerability:

PHP remote file include vulnerability in index.php for Gallery 1.4 and 1.4-pl1, when running on Windows or in Configuration mode on Unix, allows remote attackers to inject arbitrary PHP code via a URL in the GALLERY_BASEDIR parameter, a different vulnerability than CVE-2002-1412. NOTE: this issue might be exploitable only during installation, or if the administrator has not run a security script after installation.

CVE-2003-1227 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
No Description Provided	www.securityfocus.com text/html	BUGTRAQ 20031011 RE: Gallery 1.4 including file vulnerability
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF gallery-indexphp-file-include(13419)
SecurityFocus	Exploit Patch Vendor Advisory www.securityfocus.com text/html	BUGTRAQ 20031011 Gallery 1.4 including file vulnerability
Gallery index.php Remote File Include Vulnerability	Exploit Patch	BID 8814

	cve.report (archive) text/html	
No Description Provided	www.securityfocus.com text/html	BUGTRAQ 20031012 Re: Gallery 1.4 including file vulnerability

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	Gallery Project	Gallery	1.4	All	All	All
Application	Gallery Project	Gallery	1.4_pl1	All	All	All
Application	Gallery Project	Gallery	1.4	All	All	All
Application	Gallery Project	Gallery	1.4_pl1	All	All	All

cpe:2.3:a:gallery_project:gallery:1.4:*:*:*:*:*:*:*:

cpe:2.3:a:gallery_project:gallery:1.4_pl1:*:*:*:*:*:*:*:

cpe:2.3:a:gallery_project:gallery:1.4:*:*:*:*:*:*:*:

cpe:2.3:a:gallery_project:gallery:1.4_pl1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→