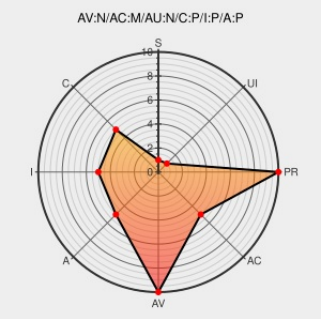
CVE-2004-1106

Published on: 12/01/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:09 PM UTC

CVE-2004-1106

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



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

Cross-site scripting (XSS) vulnerability in Gallery 1.4.4-pl3 and earlier allows remote attackers to execute arbitrary web script or HTML via "specially formed URLs," possibly via the include parameter in index.php.

CVE-2004-1106 has been assigned by cve@mitre.org to track the vulnerability

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
404 Not Found	gallery.menalto.com, text/html, Inactive Link, Not Archived	CONFIRM gallery.menalto.com/modules.php?op=modload&name=News&file=article&sid=142&mode=thread&order=0&thold=0
Gallery Unspecified Remote HTML Injection Vulnerability	Patch, Vendor Advisory, cve.report (archive), text/html	BID 11602
No Description Provided	g3cko.info, Inactive Link, Not Archived	MISC g3cko.info/gallery2-4.patch
Gentoo Linux Documentation -- Gallery: Cross-site scripting vulnerability	Patch, Vendor Advisory, www.gentoo.org, text/html	GENTOO GLSA-200411-10

Debian -- Security Information -- DSA-642-1 gallery	Patch www.debian.org Depreciated Link text/html	DEBIAN DSA-642
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF gallery-script-xss(17948)

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	1.4.1	All	All	All
Application	Gallery Project	Gallery	1.4.2	All	All	All
Application	Gallery Project	Gallery	1.4.3_pl1	All	All	All
Application	Gallery Project	Gallery	1.4.3_pl2	All	All	All
Application	Gallery Project	Gallery	1.4_pl1	All	All	All
Application	Gallery Project	Gallery	1.4_pl2	All	All	All
Application	Gallery Project	Gallery	1.4	All	All	All
Application	Gallery Project	Gallery	1.4.1	All	All	All
Application	Gallery Project	Gallery	1.4.2	All	All	All
Application	Gallery Project	Gallery	1.4.3_pl1	All	All	All
Application	Gallery Project	Gallery	1.4.3_pl2	All	All	All
Application	Gallery Project	Gallery	1.4_pl1	All	All	All
Application	Gallery Project	Gallery	1.4_pl2	All	All	All
Operating System	Gentoo	Linux	All	All	All	All
Operating System	Gentoo	Linux	All	All	All	All

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

cpe:2.3:a:gallery_project:gallery:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:gallery_project:gallery:1.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:gallery_project:gallery:1.4.3_pl1:*:*:*:*:*:*:*:

cpe:2.3:a:gallery_project:gallery:1.4.3_pl2:*:*:*:*:*:*:*:

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

cpe:2.3:a:gallery_project:gallery:1.4_pl2:*:*:*:*:*:*:*:

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

cpe:2.3:a:gallery_project:gallery:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:gallery_project:gallery:1.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:gallery_project:gallery:1.4.3_pl1:*:*:*:*:*:*:*:

cpe:2.3:a:gallery_project:gallery:1.4.3_pl2:*:*:*:*:*:*:*:

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

cpe:2.3:a:gallery_project:gallery:1.4_pl2:*:*:*:*:*:*:*:

cpe:2.3:o:gentoo:linux:*:*:*:*:*:*:*:*:

cpe:2.3:o:gentoo:linux:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→