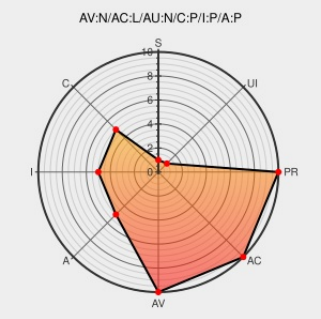
CVE-2004-1466

Published on: 12/31/2004 05:00:00 AM UTC

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

CVE-2004-1466

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



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

The set_time_limit function in Gallery before 1.4.4_p2 deletes non-image files in a temporary directory every 30 seconds after they have been uploaded using save_photos.php, which allows remote attackers to upload and execute execute arbitrary scripts before they are deleted, if the temporary directory is under the web root.

CVE-2004-1466 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
Neohapsis Archives - Full Disclosure List - #0757 - [Full-Disclosure] Gallery 1.4.4 save_photos.php PHP Insertion Proof of Concept	Exploit, web.archive.org, text/html, Inactive Link, Not Archived	FULLDISC 20040817 Gallery 1.4.4 save_photos.php PHP Insertion Proof of Concept
Gentoo Linux Documentation -- Gallery: Arbitrary command execution	Patch, www.gentoo.org, text/html	GENTOO GLSA-200409-05
Gallery 1.4.4-pl1 is now Available! | Gallery	Patch, web.archive.org, text/html	CONFIRM gallery.menalto.com/modules.php?op=modload&name=News&file=article&sid=134&mode=thread&order=0&thold=0

	Inactive Link Not Archived	
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF gallery-savephotos-file-upload(17021)
Gallery Remote Server-Side Script Execution Vulnerability	Exploit Patch cve.report (archive) text/html	BID 10968

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	1.4.4	All	All	All
Application	Gallery Project	Gallery	1.4.4	All	All	All

cpe:2.3:a:gallery_project:gallery:1.4.4:*:*:*:*:*:*:*:

cpe:2.3:a:gallery_project:gallery:1.4.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→