



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

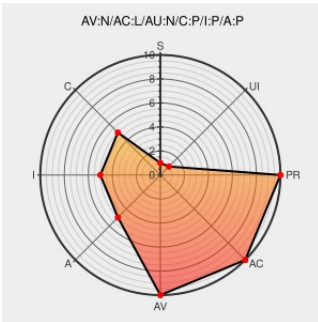
Last Modified on: 03/23/2021 11:28:11 PM UTC

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 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

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	1.4.4	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 →](#)

© CVE.report 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)