



CVE-2006-0587

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2006-0587
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-08 01:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Unspecified vulnerability in util.php in Gallery before 1.5.2-pl2 allows remote authenticated users with trick an owner into m...

Risk And Classification

Primary CVSS: v2.0 6.5 from nvd@nist.gov

AV:N/AC:L/Au:S/C:P/I:P/A:P

EPSS: 0.017440000 probability, percentile 0.825610000 (date 2026-04-16)

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:S/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	Gallery Project	Gallery	1.3.4	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	1.4.4_pl2	All	All	All
Application	Gallery Project	Gallery	1.4.4_pl3	All	All	All
Application	Gallery Project	Gallery	1.4.4_pl4	All	All	All
Application	Gallery Project	Gallery	1.4.4_pl5	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	1.5	All	All	All
Application	Gallery Project	Gallery	1.5.1	All	All	All
Application	Gallery Project	Gallery	1.5.1_rc2	All	All	All
Application	Gallery Project	Gallery	1.5.2_rc2	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference					Source	
Gallery web-based photo gallery remote file execution - Digital Armaments for Intelligence					af854a3a-2127-422b-91e6-400000000000	
Gallery 1.5.2-pl2 Security Release Gallery					af854a3a-2127-422b-91e6-400000000000	
IBM X-Force Exchange					af854a3a-2127-422b-91e6-400000000000	
www.osvdb.org/23256					af854a3a-2127-422b-91e6-400000000000	
archives.neohapsis.com/archives/bugtraq/2006-02/0224.html					af854a3a-2127-422b-91e6-400000000000	
IBM X-Force Exchange					af854a3a-2127-422b-91e6-400000000000	
archives.neohapsis.com/archives/bugtraq/2006-02/0286.html					af854a3a-2127-422b-91e6-400000000000	
Gallery Data Code Execution Vulnerability					af854a3a-2127-422b-91e6-400000000000	
www.osvdb.org/22944					af854a3a-2127-422b-91e6-400000000000	
Gallery 'util.php' Include File Bug Lets Remote Users Execute Code Stored on the Local System - SecurityTracker					af854a3a-2127-422b-91e6-400000000000	
Gallery "util.php" Local File Inclusion Vulnerability - Advisories - Secunia					af854a3a-2127-422b-91e6-400000000000	
CVE Program record					CVE.ORG	
NVD vulnerability detail					NVD	

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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