



CVE-2005-0376

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2005-0376
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-01-12 05:00:00 UTC
Updated	2017-07-11 01:32:00 UTC
Description	PHP remote file inclusion vulnerability in SGallery 1.01 allows local and possibly remote attackers to execute arbitrary PHP

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sergey Kiselev	Sgallery	1.01	All	All	All
Application	Sergey Kiselev	Sgallery	1.01	All	All	All

References

Reference

'[waraxe-2005-SA#039] - Critical Sql Injection in Sgallery module' - MARC
Secunia - Advisories - PHP-Nuke Sgallery Module File Inclusion and SQL Injection
SecurityTracker.com Archives - SGallery Input Validation Holes Let Remote Users Inject SQL Commands and Potentially Execute Arbitrary Co
Waraxe IT Security Portal
[Full-Disclosure] [waraxe-2005-SA#039] - Critical Sql Injection in Sgallery module for PhpNuke
IBM X-Force Exchange
CVE Program record
NVD vulnerability detail

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](#)