



CVE-2015-3923

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

Summary

CVE	CVE-2015-3923
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-10 18:59:00 UTC
Updated	2023-11-07 02:25:00 UTC
Description	Coppermine Photo Gallery before 1.5.36 allows remote attackers to enumerate directories via a full path in the folder param

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Coppermine-gallery	Coppermine Photo Gallery	All	All	All	All

References

Reference

- forum.coppermine-gallery.net/index.php/topic%2C78194.0.html
- Coppermine Photo Gallery Input Validation Flaw Permits Cross-Site Scripting, Browser Redirect, and Path Disclosure Attacks - SecurityTracke
- Malformed Request
- forum.coppermine-gallery.net/index.php/topic,78194.0.html
- Coppermine Gallery 1.5.34 XSS / Open Redirection ≈ Packet Storm
- 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](#)