



CVE-2006-4260

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

Summary

CVE	CVE-2006-4260
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-08-21 20:04:00 UTC
Updated	2017-07-20 01:32:00 UTC
Description	Directory traversal vulnerability in index.php in Fotopholder 1.8 allows remote attackers to read arbitrary directories or files via a crafted request.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jake Olefsky	Fotopholder	1.8	All	All	All
Application	Jake Olefsky	Fotopholder	1.8	All	All	All

References

Reference

IBM X-Force Exchange
SecurityReason - otopholder 1.8 suffers from a local file inclusion,XSS and directory listing vuln
28243
20060815 otopholder 1.8 suffers from a local file inclusion,XSS and directory listing vuln
SecurityTracker.com Archives - Fotopholder Input Validation Holes Permit Directory Traversal and Cross-Site Scripting Attacks and Let Remo
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](#)