



CVE-2006-4052

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

Summary

CVE	CVE-2006-4052
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-08-10 00:04:00 UTC
Updated	2018-10-17 21:33:00 UTC
Description	Multiple PHP remote file inclusion vulnerabilities in Turnkey Web Tools PHP Simple Shop 2.0 and earlier allow remote attac

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Turnkey Web Tools	Php Simple Shop	All	All	All	All

References

Reference	Source
IBM X-Force Exchange	XF
27802	OS
27805	OS
PHP Simple Shop "abs_path" File Inclusion Vulnerability - Advisories - Secunia	SE
PHP Simple Shop 2.0 - 'abs_path' Remote File Inclusion - PHP webapps Exploit	E
SecurityTracker.com Archives - PHP Simple Shop Include File Error in 'abs_path' Parameter Lets Remote Users Execute Arbitrary Code	SE
27800	OS
SecurityFocus	BU
27804	OS
27803	OS
Webmail- OVH	VU
27801	OS
ECHO	MI

CVE Program record

CV

NVD vulnerability detail

NV

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](#)