



CVE-2012-3354

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2012-3354
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-11-20 00:55:00 UTC
Updated	2013-12-13 05:02:00 UTC
Description	doku.php in DokuWiki, as used in Fedora 16, 17, and 18, when certain PHP error levels are set, allows remote attackers to

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dokuwiki	Dokuwiki	-	All	All	All
Application	Dokuwiki	Dokuwiki	-	All	All	All
Operating System	Fedoraproject	Fedora	16	All	All	All
Operating System	Fedoraproject	Fedora	17	All	All	All
Operating System	Fedoraproject	Fedora	18	All	All	All
Operating System	Fedoraproject	Fedora	16	All	All	All
Operating System	Fedoraproject	Fedora	17	All	All	All
Operating System	Fedoraproject	Fedora	18	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] Fedora 18 Update: dokuwiki-0-0.14.20121013.fc18	FEDORA	lists.fedoraproject.org	
oss-security - CVE request: Full path disclosure in DokuWiki	MLIST	www.openwall.com	
Bug 835145 – CVE-2012-3354 dokuwiki: Full path disclosure with PHP error level enabled	MISC	bugzilla.redhat.com	
oss-security - Re: CVE request: Full path disclosure in DokuWiki	MLIST	www.openwall.com	
[dokuwiki] Fwd: DokuWiki - Full path disclosure - dokuwiki - FreeLists	MISC	www.freelists.org	
Support / Security / Advisories // MDVSA-2013:073 Mandriva	MANDRIVA	www.mandriva.com	

[SECURITY] Fedora 16 Update: dokuwiki-0-0.14.20121013.fc16	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 17 Update: dokuwiki-0-0.14.20121013.fc17	FEDORA	lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report