



CVE-2008-2717

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

Summary

CVE	CVE-2008-2717
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-06-16 22:41:00 UTC
Updated	2018-10-11 20:42:00 UTC
Description	TYPO3 4.0.x before 4.0.9, 4.1.x before 4.1.7, and 4.2.x before 4.2.1, uses an insufficiently restrictive default fileDenyPattern

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Apache Webserver	All	All	All	All
Application	Apache	Apache Webserver	All	All	All	All
Application	Typo3	Typo3	4.0	All	All	All
Application	Typo3	Typo3	4.0.1	All	All	All
Application	Typo3	Typo3	4.0.2	All	All	All
Application	Typo3	Typo3	4.0.3	All	All	All
Application	Typo3	Typo3	4.0.4	All	All	All
Application	Typo3	Typo3	4.0.5	All	All	All
Application	Typo3	Typo3	4.0.6	All	All	All
Application	Typo3	Typo3	4.0.7	All	All	All
Application	Typo3	Typo3	4.0.8	All	All	All
Application	Typo3	Typo3	4.1	All	All	All
Application	Typo3	Typo3	4.1.1	All	All	All
Application	Typo3	Typo3	4.1.2	All	All	All
Application	Typo3	Typo3	4.1.3	All	All	All
Application	Typo3	Typo3	4.1.4	All	All	All
Application	Typo3	Typo3	4.1.5	All	All	All

Application	Typo3	Typo3	4.1.6	All	All	All
Application	Typo3	Typo3	4.2	All	All	All
Application	Typo3	Typo3	4.0	All	All	All
Application	Typo3	Typo3	4.0.1	All	All	All
Application	Typo3	Typo3	4.0.2	All	All	All
Application	Typo3	Typo3	4.0.3	All	All	All
Application	Typo3	Typo3	4.0.4	All	All	All
Application	Typo3	Typo3	4.0.5	All	All	All
Application	Typo3	Typo3	4.0.6	All	All	All
Application	Typo3	Typo3	4.0.7	All	All	All
Application	Typo3	Typo3	4.0.8	All	All	All
Application	Typo3	Typo3	4.1	All	All	All
Application	Typo3	Typo3	4.1.1	All	All	All
Application	Typo3	Typo3	4.1.2	All	All	All
Application	Typo3	Typo3	4.1.3	All	All	All
Application	Typo3	Typo3	4.1.4	All	All	All
Application	Typo3	Typo3	4.1.5	All	All	All
Application	Typo3	Typo3	4.1.6	All	All	All
Application	Typo3	Typo3	4.2	All	All	All

References				
Reference	Source	Link		
Debian -- Security Information -- DSA-1596-1 typo3	DEBIAN	www.debian.org		
TYPO3 File Upload and Cross-Site Scripting Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.ovh.com		
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com		
SecurityReason - Multiple vulnerabilities in TYPO3 Core	SREASON	secunia.com		
SecurityFocus	BUGTRAQ	www.securityfocus.com		
Debian update for typo3 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com		
buzz.typo3.org: Advice on core security issue regarding fileDenyPattern	CONFIRM	buzz.typo3.org		
typo3.org: TYPO3 Security Bulletin TYPO3-20080611-1: Multiple vulnerabilities in TYPO3 Core	CONFIRM	typo3.org		
TYPO3 Cross-Site Scripting Vulnerability and File Upload Vulnerability	BID	www.bidsa.org		
CVE Program record	CVE.ORG	www.cve.org		
NVD vulnerability detail	NVD	nvd.nist.gov		

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](#)