



CVE-2005-0294

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

Summary

CVE	CVE-2005-0294
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-01-16 05:00:00 UTC
Updated	2017-07-11 01:32:00 UTC
Description	minis.php in Minis 0.2.1 allows remote attackers to cause a denial of service (infinite loop) via an HTTP request for a file tha

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Minis	Minis	0.2.1	All	All	All
Application	Minis	Minis	0.2.1	All	All	All

References

Reference	Source	Link	Tags
[Full-Disclosure] Minis directory traversal vulnerability	FULLDISC	lists.grok.org.uk	Exploit, Ver
SecurityTracker.com Archives - Minis Discloses Certain Files to Remote Users	SECTRAK	securitytracker.com	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
Secunia - Advisories - Minis "month" Directory Traversal Vulnerability	SECUNIA	secunia.com	
'Minis directory traversal vulnerability' - MARC	BUGTRAQ	marc.info	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, e

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](#)