



CVE-2004-2526

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2526

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Tivoli Directory Server](#) from [Ibm](#) contain the following vulnerability:

Directory traversal vulnerability in Idacgi.exe in IBM Tivoli Directory Server 4.1 and earlier allows remote attackers to view arbitrary files via a .. (dot dot) in the Template parameter.

CVE-2004-2526 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

Secunia - Advisories - IBM Tivoli Directory Server Cross-Site Scripting and Directory Traversal Vulnerabilities

[Exploit](#)
[Patch](#)
[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[X SECUNIA 10347](#)

Neohapsis Archives - Full Disclosure List - #1311 - [Full-Disclosure] IBM Directory Server - Idacgi.exe

[Exploit](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[FULLDISC 20040802 IBM Directory Server - Idacgi.exe](#)

[Exploit](#)
[Patch](#)
[Vendor Advisory](#)
[www.oliverkarow.de](#)
[text/plain](#)

[MISC](#)
[www.oliverkarow.de/research/IDS_directory_traversal.txt](#)

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF tivoli-directory-directory-traversal(16850)
IBM notice: The page you requested cannot be displayed	Patch Vendor Advisory www-1.ibm.com text/html Inactive Link Not Archived	 AIXAPAR IR53631
IBM Tivoli Directory Server LDACGI Directory Traversal Vulnerability	Vendor Advisory cve.report (archive) text/html	 BID 10841
IBM Directory Server 'ldacgi' Discloses Files to Remote Users - SecurityTracker	Exploit Patch Vendor Advisory securitytracker.com text/html	 SECTRAK 1010831
IBM notice: The page you requested cannot be displayed	Patch Vendor Advisory www-1.ibm.com text/html Inactive Link Not Archived	 AIXAPAR IR52692
No Description Provided	Exploit Patch Vendor Advisory www.osvdb.org Inactive Link Not Archived	 OSVDB 8367

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Tivoli Directory Server	3.2.2	All	All	All
Application	Ibm	Tivoli Directory Server	3.2.2	All	All	All
Application	Ibm	Tivoli Directory Server	All	All	All	All
cpe:2.3:a:ibm:tivoli_directory_server:3.2.2:*:*:*:*:*:						
cpe:2.3:a:ibm:tivoli_directory_server:3.2.2:*:*:*:*:*:						
cpe:2.3:a:ibm:tivoli_directory_server:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)