



# CVE-2010-0312

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

## Summary

<b>CVE</b>	CVE-2010-0312
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2010-01-14 19:30:00 UTC
<b>Updated</b>	2026-04-23 00:35:47 UTC
<b>Description</b>	The do_extendedOp function in ibmslapd in IBM Tivoli Directory Server (TDS) 6.2 on Linux allows remote attackers to caus

## Risk And Classification

**Primary CVSS:** v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

**Problem Types:** CWE-20 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None


Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Tivoli Directory Server	6.2	All	All	All

Operating System	Linux	Linux Kernel	All	All	All	All
<b>Vendor Declared Affected Products</b>						
<b>Source</b>	<b>Vendor</b>	<b>Product</b>	<b>Version</b>	<b>Platforms</b>		
CNA	Na	N/a	affected n/a	Not specified		
<b>References</b>						
<b>Reference</b>				<b>Source</b>		
Intevydis blog: Tivoli Directory Server 6.2 do_extendedOp DoS				af854a3a-2127-422b-91ae-364		
IBM Tivoli Directory Server Null Pointer Dereference Lets Remote Users Crash the Server - SecurityTracker				af854a3a-2127-422b-91ae-364		
CVE Program record				CVE.ORG		
NVD vulnerability detail				NVD		
						
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](#)