



CVE-2005-3567

Published on: 11/16/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

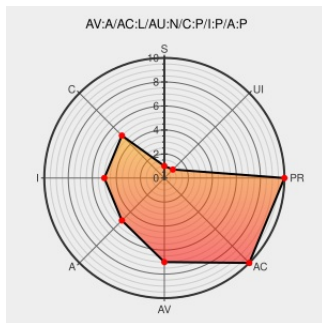
CVE-2005-3567

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Tivoli Directory Server** from **ibm** contain the following vulnerability:

slapd daemon in IBM Tivoli Directory Server (ITDS) 5.2.0 and 6.0.0 binds using SASL EXTERNAL, which allows attackers to bypass authentication and modify and delete directory data via unknown attack vectors.

CVE-2005-3567 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: **5.8 - MEDIUM**

Access
Vector

ADJACENT_NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

IBM Tivoli Directory Server
Unspecified Unauthorized
Access Vulnerability

[Patch](#)
[cve.report \(archive\)](#)
[text/html](#)

[BID 15367](#)

Search results

[www-1.ibm.com](#)
[text/html](#)

[AIXAPAR IO02714](#)

No Description Provided

[Patch](#)
[www.osvdb.org](#)

[OSVDB 20672](#)

Inactive Link **Not Archived**

IBM notice: The page you
requested cannot be
displayed

[www-1.ibm.com](#)
[text/html](#)
Inactive Link **Not Archived**

[CONFIRM www-1.ibm.com/support/docview.wss?uid=isg1SSRVAIX53SECUR081510_247](#)

Search results

[www-1.ibm.com](#)

[AIXAPAR IO02697](#)

	text/html	
IBM notice: The page you requested cannot be displayed	Patch Vendor Advisory www-1.ibm.com text/html Inactive Link Not Archived	 CONFIRM www-1.ibm.com/support/docview.wss?rs=767&context=SSVJJU&dc=D400&uid=swg24010819&loc=en_US&cs=UTF-8&lang=en
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	 VUPEN ADV-2005-2356
Secunia - Advisories - IBM Tivoli Directory Server Unspecified Security Bypass Vulnerability	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 17484
US-CERT Vulnerability Note VU#194753	US Government Resource www.kb.cert.org text/html	 CERT-VN VU#194753
IBM notice: The page you requested cannot be displayed	Patch Vendor Advisory www-1.ibm.com text/html Inactive Link Not Archived	 CONFIRM www-1.ibm.com/support/docview.wss?uid=swg21222159
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF tivoli-directory-bypass-security(22989)
SecurityTracker.com Archives - IBM Tivoli Directory Server Unspecified SLAPD Binding Error May Let Remote Users Modify/Delete Data	Patch securitytracker.com text/html	 SECTrack 1015171
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	5.2.0	All	All	All
Application	IBM	Tivoli Directory Server	6.0	All	All	All
Application	IBM	Tivoli Directory Server	5.2.0	All	All	All
Application	IBM	Tivoli Directory Server	6.0	All	All	All
cpe:2.3:a:ibm:tivoli_directory_server:5.2.0:*:*:*:*:*:						
cpe:2.3:a:ibm:tivoli_directory_server:6.0:*:*:*:*:*:						
cpe:2.3:a:ibm:tivoli_directory_server:5.2.0:*:*:*:*:*:						

cpe:2.3:a:ibm:tivoli_directory_server:6.0:*:*:*:*:*:*:

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](#)