



CVE-2012-0726

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

Summary

CVE	CVE-2012-0726
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-04-22 18:55:00 UTC
Updated	2017-12-19 02:29:00 UTC
Description	The default configuration of TLS in IBM Tivoli Directory Server (TDS) 6.3 and earlier supports the (1) NULL-MD5 and (2) NULL

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Tivoli Directory Server	3.2.2	All	All	All
Application	ibm	Tivoli Directory Server	4.1	All	All	All
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	6.0.0	All	All	All
Application	ibm	Tivoli Directory Server	6.0.0.69	All	All	All
Application	ibm	Tivoli Directory Server	6.0.0.7	All	All	All
Application	ibm	Tivoli Directory Server	6.0.0.8	All	All	All
Application	ibm	Tivoli Directory Server	6.1.0	All	All	All
Application	ibm	Tivoli Directory Server	6.1.0.45	All	All	All
Application	ibm	Tivoli Directory Server	6.1.0.46	All	All	All
Application	ibm	Tivoli Directory Server	6.1.0.47	All	All	All
Application	ibm	Tivoli Directory Server	6.1.0.48	All	All	All
Application	ibm	Tivoli Directory Server	6.2.0	All	All	All
Application	ibm	Tivoli Directory Server	6.2.0.19	All	All	All
Application	ibm	Tivoli Directory Server	6.2.0.20	All	All	All
Application	ibm	Tivoli Directory Server	6.2.0.21	All	All	All

Application	Ibm	Tivoli Directory Server	6.2.0.22	All	All	All
Application	Ibm	Tivoli Directory Server	3.2.2	All	All	All
Application	Ibm	Tivoli Directory Server	4.1	All	All	All
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	6.0.0	All	All	All
Application	Ibm	Tivoli Directory Server	6.0.0.69	All	All	All
Application	Ibm	Tivoli Directory Server	6.0.0.7	All	All	All
Application	Ibm	Tivoli Directory Server	6.0.0.8	All	All	All
Application	Ibm	Tivoli Directory Server	6.1.0	All	All	All
Application	Ibm	Tivoli Directory Server	6.1.0.45	All	All	All
Application	Ibm	Tivoli Directory Server	6.1.0.46	All	All	All
Application	Ibm	Tivoli Directory Server	6.1.0.47	All	All	All
Application	Ibm	Tivoli Directory Server	6.1.0.48	All	All	All
Application	Ibm	Tivoli Directory Server	6.2.0	All	All	All
Application	Ibm	Tivoli Directory Server	6.2.0.19	All	All	All
Application	Ibm	Tivoli Directory Server	6.2.0.20	All	All	All
Application	Ibm	Tivoli Directory Server	6.2.0.21	All	All	All
Application	Ibm	Tivoli Directory Server	6.2.0.22	All	All	All
Application	Ibm	Tivoli Directory Server	All	All	All	All

References

Reference

Security Bulletin: IBM Tivoli Directory Server use of NULL ciphers in default Transport Layer Security configuration would result in unencrypted

IBM notice: The page you requested cannot be displayed

IBM X-Force Exchange

IBM Tivoli Directory Server Multiple Security Vulnerabilities

IBM notice: The page you requested cannot be displayed

IBM Tivoli Directory Server NULL Ciphers Let Remote Users Obtain Potentially Sensitive Information - SecurityTracker

IBM notice: The page you requested cannot be displayed

CVE Program record

NVD vulnerability detail

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](#)