



CVE-2006-0451

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2006-0451
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-14 22:06:00 UTC
Updated	2017-07-20 01:29:00 UTC
Description	Multiple memory leaks in the LDAP component in Fedora Directory Server 1.0 allow remote attackers to cause a denial of s

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Fedora Core	1.0	All	directory_server	All
Operating System	Redhat	Fedora Core	1.0	All	directory_server	All

References

Reference	Source
Fedora Directory Server Multiple Remote Denial Of Service Vulnerabilities	BID
Secunia - Advisories - Fedora Directory Server LDAP Denial of Service Vulnerabilities	SECUNIA
IBM X-Force Exchange	XF
179135 – (CVE-2006-0451) CVE-2006-0451 memory leaks using ber_scanf when handling bad BER packets (CVE-2006-0453)	CONFIRM
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](#).

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