



# CVE-2008-1677

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

## Summary

<b>CVE</b>	CVE-2008-1677
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-05-12 16:20:00 UTC
<b>Updated</b>	2022-02-03 19:56:00 UTC
<b>Description</b>	Buffer overflow in the regular expression handler in Red Hat Directory Server 8.0 and 7.1 before SP6 allows remote attacks

## Risk And Classification

### Problem Types: CWE-120

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Redhat</a>	<a href="#">Directory Server</a>	7.1	sp1	All	All
Application	<a href="#">Redhat</a>	<a href="#">Directory Server</a>	7.1	sp2	All	All
Application	<a href="#">Redhat</a>	<a href="#">Directory Server</a>	7.1	sp3	All	All
Application	<a href="#">Redhat</a>	<a href="#">Directory Server</a>	7.1	sp4	All	All
Application	<a href="#">Redhat</a>	<a href="#">Directory Server</a>	7.1	sp5	All	All
Application	<a href="#">Redhat</a>	<a href="#">Directory Server</a>	8.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Directory Server</a>	7.1	sp1	All	All
Application	<a href="#">Redhat</a>	<a href="#">Directory Server</a>	7.1	sp2	All	All
Application	<a href="#">Redhat</a>	<a href="#">Directory Server</a>	7.1	sp3	All	All
Application	<a href="#">Redhat</a>	<a href="#">Directory Server</a>	7.1	sp4	All	All
Application	<a href="#">Redhat</a>	<a href="#">Directory Server</a>	7.1	sp5	All	All
Application	<a href="#">Redhat</a>	<a href="#">Directory Server</a>	8.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Fedora Directory Server</a>	1.1	All	All	All
Application	<a href="#">Red Hat</a>	<a href="#">Fedora Directory Server</a>	1.1	All	All	All
Application	<a href="#">Red Hat</a>	<a href="#">Fedora Directory Server</a>	1.1	All	All	All

## References

Reference	Source	Li
Fedora Directory Server Regular Expression Handler Buffer Overflow - Advisories - Secunia	SECUNIA	<a href="#">se</a>
444712 – (CVE-2008-1677) CVE-2008-1677 Directory Server: insufficient buffer size for search patterns	MISC	<a href="#">bu</a>
Red Hat Directory Server LDAP Query Patterns Buffer Overflow Vulnerability	BID	<a href="#">wv</a>
Support	REDHAT	<a href="#">wv</a>
Red Hat Directory Server Buffer Overflow in Regex Handler Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="#">wv</a>
Red Hat Directory Server Regular Expression Handler Buffer Overflow - Advisories - Secunia	SECUNIA	<a href="#">se</a>
Support	REDHAT	<a href="#">wv</a>
IBM X-Force Exchange	XF	<a href="#">ex</a>
CVE Program record	CVE.ORG	<a href="#">wv</a>
NVD vulnerability detail	NVD	<a href="#">nv</a>

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](#)**