



CVE-2007-6701

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

Summary

CVE	CVE-2007-6701
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-02-13 21:00:00 UTC
Updated	2017-08-08 01:29:00 UTC
Description	Multiple stack-based buffer overflows in the Spooler service (nwspool.dll) in Novell Client 4.91 SP4 for Windows allow remo

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Application	Novell	Client	4.91	sp4	All	All
Application	Novell	Client	4.91	sp4	All	All

References

Reference	Source	L
Novell Client NWSPool.DLL Unspecified Buffer Overflow Vulnerability	BID	w
Novell Client 4.91 Post-SP4 NWSPool.DLL	CONFIRM	SI
SecurityTracker.com Archives - Novell Client 'NWSPool.DLL' Stack Overflow Lets Remote Users Execute Arbitrary Code	SECTRAK	sc
Novell Client NWSPool.DLL Buffer Overflow Vulnerability - Advisories - Secunia	SECUNIA	sc
20070806 ZDI-07-045: Novell Client NWSPool.DLL Stack Overflow Vulnerability	BUGTRAQ	al
ZDI-07-045	MISC	w
IBM X-Force Exchange	XF	e:
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n'

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](#)