



CVE-2008-0639

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

Summary

CVE	CVE-2008-0639
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-02-13 21:00:00 UTC
Updated	2018-10-15 22:02:00 UTC
Description	Stack-based buffer overflow in the EnumPrinters function in the Spooler service (nwspool.dll) in Novell Client 4.91 SP2, SP3, SP4, and SP5; a remote attacker could exploit this vulnerability to execute arbitrary code on the target system.

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	sp2	All	All
Application	Novell	Client	4.91	sp3	All	All
Application	Novell	Client	4.91	sp4	All	All
Application	Novell	Client	4.91	sp2	All	All
Application	Novell	Client	4.91	sp3	All	All
Application	Novell	Client	4.91	sp4	All	All

References

Reference
Downloads
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
'[Full-disclosure] ZDI-08-005: Novell Client NWSPOOL.DLL' - MARC
SecurityFocus
Novell Client NWSPOOL.DLL "EnumPrinters()" Buffer Overflow - Secunia Advisories - Vulnerability Intelligence - Secunia.com
SecurityTracker.com Archives - Novell Client NWSPOOL.DLL Stack Overflow in EnumPrinters() Let Remote Users Execute Arbitrary Code

Zero Day Initiative
Novell Client 4.91 Post-SP2/3/4 NWSPool.DLL 2
Novell Client 'nwspool.dll' EnumPrinters RPC Request Buffer Overflow Vulnerability
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](#)