

# [NT] Novell Client NWSPOOL.DLL EnumPrinters Stack Overflow Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-02/msg00046.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 13 Feb 2008 12:07:09 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Novell Client NWSPOOL.DLL EnumPrinters Stack Overflow Vulnerability

---

## SUMMARY

A vulnerability allows remote attackers to execute arbitrary code on systems with vulnerable installations of the Novell Netware Client. Authentication is not required to exploit this vulnerability.

## DETAILS

Vulnerable Systems:

- \* Novell Client version 4.91 SP2
- \* Novell Client version 4.91 SP3
- \* Novell Client version 4.91 SP4

The specific flaw exists in nwsPOOL.dll which is responsible for handling RPC requests through the spoolss named pipe. The EnumPrinters function exposed by this DLL contains a logical flaw allowing an attacker to bypass a patch introduced to prevent the vulnerability described in ZDI-07-045. Exploitation of this vulnerability leads to arbitrary code execution in the context of the SYSTEM user.

Vendor Response:

[NT] Novell Client NWSPOOL.DLL EnumPrinters Stack Overflow Vulnerability

Novell has issued an update to correct this vulnerability. More details can be found at:

<<http://download.novell.com/Download?buildid=SszG22IugM~>>  
<http://download.novell.com/Download?buildid=SszG22IugM~>

Disclosure Timeline:

2007.12.11 – Vulnerability reported to vendor  
2008.02.11 – Coordinated public release of advisory

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0639>>  
CVE-2008-0639

ADDITIONAL INFORMATION

The information has been provided by <<mailto:zdi-disclosures@xxxxxxxx>>  
The Zero Day Initiative (ZDI).  
The original article can be found at:  
<<http://www.zerodayinitiative.com/advisories/ZDI-08-005.html>>  
<http://www.zerodayinitiative.com/advisories/ZDI-08-005.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.  
To unsubscribe from the list, send mail with an empty subject line and body to:  
list-unsubscribe@xxxxxxxxxxxxxxxxx  
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====  
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.  
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.