

# [NT] Novell eDirectory DOS Device Name DoS

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-06/0054.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 06/15/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 15 Jun 2005 11:06:07 +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 eDirectory DOS Device Name DoS

---

## SUMMARY

Novell <<http://www.novell.com/products/edirectory/>> eDirectory is "a Lightweight Directory Access Protocol (LDAP)-enabled, directory-based identity management system".

Novell's eDirectory is vulnerable to denial of service whenever a DOS device name is requested from server.

## DETAILS

Vulnerable Systems:

\* Novell eDirectory version 8.7.3 (NT65DE.exe)

Requesting "DOS Device in Path Name" Denial of Service:

The problem exhibits itself when requesting an URL that includes reserved MS-DOS devices. These represent devices such as the first printer port (LPT1) and the first serial communication port (COM1).

Reserved MS-DOS device names include (partial list):

AUX, CON ,PRN, COM1 and LPT1.

Proof of concept:

Securiteam: [NT] Novell eDirectory DOS Device Name DoS

<http://target:8008/COM1>

<http://target:8008/COM2>

<http://target:8008/AUX>

Default open web-ports:

8008 HTTP

8010 HTTPS

When the attack is performed the service will stop, until manually restarted

Patch Availability:

Apply the current interim release for eDirectory 8.7.3 available on the

<<http://support.novell.com/novell>> <http://support.novell.com/novell>

Disclosure Timeline:

- \* 08.01.05 – Vulnerability discovered
- \* 17.04.05 – Research ended
- \* 18.04.05 – Novell Notified (secure@novell.com)
- \* 18.04.05 – Received response from Ed Reed, Security Tzar, Novell, Inc.
- \* 03.06.05 – Novell Fixes issue
- \* 13.06.05 – Public Release

ADDITIONAL INFORMATION

The information has been provided by <mailto:advisory@cirt.dk> Dennis Rand.

The original article can be found at:

<<http://www.cirt.dk/advisories/cirt-33-advisory.pdf>>

<http://www.cirt.dk/advisories/cirt-33-advisory.pdf>

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.