

# [NEWS] Legato NetWorker Log File Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0088.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 01/16/02

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Date: Wed, 16 Jan 2002 21:03:32 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Legato NetWorker Log File Vulnerability

---

## SUMMARY

<<http://portal1.legato.com/products/networker/>> Legato NetWorker is a data storage solution for enterprise environments. A security vulnerability in the product allows a local attacker to compromise the application's username and password.

## DETAILS

Vulnerable systems:

NetWorker version 6.1

Immune systems:

NetWorker version 6.1.1

The following scenario will illustrate the problem:

If Legato NetWorker is set to have one of its drives as an NDMP for use by NetApp, whenever a backup is started NetApp will store inside the `/nsr/logs/daemon.log` file all the current information. This includes sensitive information such as the username and password (in clear text) for the NetApp server. This username is usually root, or root equivalent user.

## Securiteam: [NEWS] Legato NetWorker Log File Vulnerability

Since any one can read this file, anyone with local user access would potentially be able to elevate his privileges.

Example log file:

```
01/08/02 10:20:40 nsrd: savegroup info: starting netapp (with 1 client(s))
  application information: HIST=y;
    auth index: netapp;
  auth index name space: backup, 1;
    auth level: full;
    auth mode: save;
    auth server: server;
    auth sname: /vol/vol0;
  auth sname long: /vol/vol0;
    auth sstime: 10xxxxxx;
  auth sstime 64-bit: 10xxxxxx;
  client id: \
xxxxxxxxxxxxxxxx;
    groups: netapp;
  hard session limit: 1;
  hostname: server;
  locale: C;
  ndmp: Yes;
  password: password;
  remote user: root;
  store index entries: Yes;
  volume pool: netapp;
```

Solution:

A newer version of NetWorker solves this problem.

Workaround:

Manually change the permissions of the /nsr/logs directory to 0700.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[vsira@hotmail.com](mailto:vsira@hotmail.com)> Venkatesh babu Sira and <mailto:[wf227@yahoo.de](mailto:wf227@yahoo.de)> Wolfgang Fischer.

=====

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](mailto:list-unsubscribe@securiteam.com)

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

---

- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[\[NT\] Pi3Web Webserver Buffer Overflow Vulnerability](#)"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)