

# [NT] EMC Legato Networker DoS and Multiple Buffer Overflows

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00067.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 19 Jan 2006 17:04:18 +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>

-----

EMC Legato Networker DoS and Multiple Buffer Overflows

---

## SUMMARY

"The <<http://www.legato.com/products/networker/index.htm>> EMC NetWorker family is the fastest and most flexible backup and recovery solution in the industry."

Multiple buffer overflows and a DoS allow attackers to execute arbitrary code and crash EMC Legato Networker.

## DETAILS

### Vulnerable Systems:

- \* EMC Legato Networker version 7.2 build 172

### Immune Systems:

- \* EMC Legato NetWorker version 7.1.4
- \* EMC Legato NetWorker version 7.3

### nsrd.exe Buffer Overflow:

The vulnerability specifically exists due to improper handling of malformed RPC requests to RPC program number 390109. When such a request

## [NT] EMC Legato NetWorker DoS and Multiple Buffer Overflows

is sent by an attacker, it is possible to overwrite portions of heap memory, thus leading to arbitrary code execution.

Successful exploitation allows a remote attacker to gain access to a targeted machine. As nsrd.exe is installed on backup client machines and server machines, an attacker may rapidly compromise a network using this vulnerability.

Remote exploitation of a heap overflow vulnerability in EMC Legato NetWorker allow attackers to execute arbitrary code on Windows platforms.

nsrexecd.exe Buffer Overflow:

The vulnerability specifically exists due to improper handling of malformed RPC requests to RPC program number 390113. When such a request is sent by an attacker, it is possible to overwrite portions of heap memory, thus leading to arbitrary code execution by way of a function pointer overwrite. If an attacker can populate memory so that his data is in a predictable location, arbitrary code execution is possible. It is possible to populate memory in several ways, including by utilizing memory leaks.

Successful exploitation allows a remote attacker to gain access to a targeted machine. As nsrd.exe is installed on backup client machines as well as server machines, an attacker may rapidly compromise a network using this vulnerability.

Remote exploitation of a heap overflow vulnerability in EMC Legato NetWorker allows attackers to execute arbitrary code on windows platforms.

nsrd.exe DoS:

The vulnerability specifically exists due to improper handling of malformed RPC requests to RPC program number 390109. By sending such a request, an attacker is able to cause a NULL pointer to be used as the base in a memory reference, which leads to a crash of the service. The daemon will crash on a NULL pointer dereference as no exception handlers are invoked which might allow it to recover.

Successful exploitation allows a remote attacker to crash the nsrd.exe process.

Remote exploitation of a denial of service vulnerability in EMC Legato NetWorker allow attackers to crash the nsrd service.

Vendor Status:

"Complete resolutions to the vulnerabilities are available today in NetWorker 7.1.4 and 7.3. EMC has created a hot-fix to protect against vulnerabilities for 7.2.1 customers. No fixes are planned for previous NetWorker releases.

These remedies are available for download at:

[http://www.legato.com/support/websupport/product\\_alerts/011606\\_NW.htm](http://www.legato.com/support/websupport/product_alerts/011606_NW.htm)

[NT] EMC Legato Networker DoS and Multiple Buffer Overflows

[http://www.legato.com/support/websupport/product\\_alerts/011606\\_NW.htm](http://www.legato.com/support/websupport/product_alerts/011606_NW.htm)

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3658>  
CAN-2005-3658

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3659>  
CAN-2005-3659

Disclosure Timeline:

11/17/2005 Initial vendor notification

11/17/2005 Initial vendor response

01/17/2006 Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by

<mailto:idlabs-advisories@xxxxxxxxxxxxxxxxxxxxx> iDEFENSE Labs.

The original article can be found at:

<http://www.odefense.com/intelligence/vulnerabilities/display.php?id=373>

<http://www.odefense.com/intelligence/vulnerabilities/display.php?id=373>

<http://www.odefense.com/intelligence/vulnerabilities/display.php?id=374>

<http://www.odefense.com/intelligence/vulnerabilities/display.php?id=374>

<http://www.odefense.com/intelligence/vulnerabilities/display.php?id=375>

<http://www.odefense.com/intelligence/vulnerabilities/display.php?id=375>

=====

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@xxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxxxx)

=====

=====

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.

- 
- Prev by Date: [\[NEWS\] Cisco Systems IOS 11 Web Service CDP Status Page Code Injection](#)
  - Next by Date: [\[NT\] Mozilla Thunderbird Attachment Spoofing Vulnerability](#)
  - Previous by thread: [\[NEWS\] Cisco Systems IOS 11 Web Service CDP Status Page Code Injection](#)
  - Next by thread: [\[NT\] Mozilla Thunderbird Attachment Spoofing Vulnerability](#)

## [NT] EMC Legato Networker DoS and Multiple Buffer Overflows

- Index(es):
  - ◆ *Date*
  - ◆ *Thread*