

# [NT] BrightStor ARCserve Backup for Laptops and Desktops DoS

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00005.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 4 Feb 2007 17:06:33 +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>

-----  
BrightStor ARCserve Backup for Laptops and Desktops DoS  
-----

## SUMMARY

"BrightStor <<http://www3.ca.com/solutions/Product.aspx?ID=263>> ARCserve Backup for Laptops & Desktops reduces business risk by providing a fast, automatic and transparent solution for backing up and restoring data on remote and mobile Windows-based PCs."

By sending a specially crafted series of packets to the LGSERVER.EXE process that listens on TCP port 2200, it is possible to cause the process to terminate.

## DETAILS

Vulnerable Systems:

- \* BrightStor ARCserve Backup for Laptops & Desktops r11.1

During the authentication negotiation, the third client packet at HEX address (DWORD) 0x11 – 0x14 in the third client packet specifies a data length. Setting this value to 0xff 0xff 0xff 0xff causes a read access violation to occur, terminating the process.

[NT] BrightStor ARCserve Backup for Laptops and Desktops DoS

Fix:

<http://supportconnectw.ca.com/public/sams/lifeguard/infodocs/babldimpsec-notice.asp>  
<http://supportconnectw.ca.com/public/sams/lifeguard/infodocs/babldimpsec-notice.asp>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:mark@xxxxxxxxxxx>> mark.

=====

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

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

=====

=====

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.