

# Re: [Full-disclosure] Invalid memory access in Acronis True Image Group Server 1.5.19.191

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-03/msg00176.html>

- *From:* Dmitry <[security.research.labs@xxxxxxxxxx](mailto:security.research.labs@xxxxxxxxxx)>
- *Date:* Tue, 11 Mar 2008 00:32:05 +0200

Oh man you are a super star !!! but why no fix ???

On Mon, Mar 10, 2008 at 11:47 PM, Luigi Auriemma <[aluigi@xxxxxxxxxxxxxxxx](mailto:aluigi@xxxxxxxxxxxxxxxx)> wrote:

#####

Luigi Auriemma

Application: Acronis True Image Group Server

<http://www.acronis.com/enterprise/products/ATIES/group-server.html>

Versions: <= 1.5.19.191  
 (included in Acronis True Image Enterprise Server  
 9.5.0.8072 and the other True Image packages)  
 Platforms: Windows  
 Bug: invalid memory access  
 Exploitation: remote  
 Date: 08 Mar 2008  
 Author: Luigi Auriemma  
 e-mail: [aluigi@xxxxxxxxxxxxxxxx](mailto:aluigi@xxxxxxxxxxxxxxxx)  
 web: [aluigi.org](http://aluigi.org)

#####

- 1) Introduction
- 2) Bug
- 3) The Code
- 4) Fix

#####

=====

1) Introduction

=====

Acronis Group Server is a component of Acronis True Image Echo Server (Workstation and Enterprise packages) which "allows the viewing and managing of backup tasks for all systems in the network from the Acronis Management Console".

#####

=====

2) Bug

=====

The packets used by this server contain some 16 bit fields which specify the length of the subsequent data. The problem is that the memory assigned for each packet is about 2048 bytes so the server allocates the amount of memory specified by that 16 bit field and then tries to copy the data from the packet into this new buffer with the subsequent crash of the service due to an invalid read access.

#####

=====

3) The Code

=====

<http://aluigi.org/poc/acrogroup.txt>

nc SERVER 9877 -v -v -u -p 9876 < acrogroup.txt

#####