

[Full-disclosure] NULL pointer in Ventrilo 3.0.2

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-08/msg00297.html>

- *From:* Luigi Auriemma <aluigi@xxxxxxxxxxxxx>
 - *Date:* Wed, 13 Aug 2008 19:13:12 +0100
-

#####

Luigi Auriemma

Application: Ventrilo

<http://www.ventrilo.com>

Versions: <= 3.0.2

Platforms: Windows, Linux i386, Solaris SPARC, Solaris x86, FreeBSD

i386, NetBSD i386, Mac OSX PowerPC

Bug: NULL pointer

Exploitation: remote, versus server

Date: 13 Aug 2008

Authors: Andre Malm Luigi Auriemma

web: sheepa.org e-mail: aluigi@xxxxxxxxxxxxx

web: aluigi.org

#####

1) Introduction

2) Bug

3) The Code

4) Fix

#####

=====

1) Introduction

=====

Ventrilo is one of the most known and used voice chat softwares for gamers.

#####

=====
2) Bug
=====

Despite the vice of the Ventrilo developers of changing the protocol of their application enough often (like the recent senseless additional encryption keys located on their centralized servers needed for the handshake and the in-game packets of the 3.x servers), the first packet sent to a Ventrilo server has ever the same format on any new and old version: type 0, version and two random strings.

If the server receives a version string different than its one it sends an "Incompatible version" error message to the client and skips the instructions that create the random keys used for the encryption and decryption of all the subsequent packets.

So if an attacker supplies an invalid version and sends another packet with any content in it, the server crashes due to the key assigned for the decryption of the client's packets which is still uninitialized (in fact the NULL pointer exception happens just in the decryption function).

#####

=====
3) The Code
=====

<http://aluigi.org/poc/ventrilobotomy.zip>

#####

=====
4) Fix
=====

No official fix.

I have written an universal work-around which works with any version and platform (SPARC and Mac OSX excluded) of the dedicated server:

<http://aluigi.org/patches/ventrilobotomyfix.zip>

#####

Luigi Auriemma

<http://alugi.org>

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>