

Multiple vulnerabilities in Toribash 2.71

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-08/msg00300.html>

- *From:* Luigi Auriemma <aluigi@xxxxxxxxxxxxx>
 - *Date:* Sun, 19 Aug 2007 00:06:26 +0200
-

#####

Luigi Auriemma

Application: Toribash
<http://www.toribash.com>
Versions: <= 2.71
Platforms: Windows, Mac and Linux
Bugs: A] dedicated server format string
B] client commands buffer-overflow
C] client unicode buffer-overflow in the SAY command
D] server crash through uninitialized values
E] line-feed dropping
F] Windows dedicated server hell bell
G] clients kicked by malformed packet
Exploitation: A, D and F versus server
B locally versus clients
all the others remotely versus clients using servers as
"bridge" for the attacks (the attacker acts as a client)
Date: 17 Aug 2007
Author: Luigi Auriemma
e-mail: aluigi@xxxxxxxxxxxxx
web: aluigi.org

#####

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

#####

- =====
- 1) Introduction

Multiple vulnerabilities in Toribash 2.71

=====

Toribash is a turn-based multiplayer game in which two players fight using violent puppets.

The game servers naturally support spectators and there are some official and non-official leagues and championship for this game, other than some mods for emulating specific martial arts.

#####

=====

2) Bugs

=====

----- A] dedicated server format string -----

A format string vulnerability is exploitable when a client enters in the match, in this occasion a string containing "BOUT ID; 1 0 0 0 0 NICKNAME 0" is passed directly to `vfprintf()`, so the nickname of the client, limited to 32 chars, can be used by an attacker as format argument.

----- B] client commands buffer-overflow -----

A buffer-overflow is located in the client's function which reads the game commands.

The problem is caused by the calling of `scanf()` with the format string "%s %i" and an output buffer of about 256 bytes.

This bug can be exploited in two different ways:

– locally using a malicious replay file