

Re: TrackMania Demo Denial of Service

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-02/0234.html>

From: Luigi Auriemma (aluigi_at_altervista.org)

Date: 02/09/04

Date: Mon, 9 Feb 2004 22:06:54 +0000

To: webmaster@securiteinfo.com, bugtraq@securityfocus.com

- > *TrackMania Demo Denial of Service*
- > *The original document can be found at*
- > <http://www.securiteinfo.com/attaques/hacking/trackmaniadoss.shtml>

Also Virtual Skipper 3 is vulnerable so the problem is in the game engine developed by Nadeo (<http://www.nadeo.com>)

- > *The multiplayer game use TCP port 2350 to communicate. If you send some*
- > *garbage to this port, it will shutdown the game server.*

Not exactly garbage data but too long values, in fact the game uses 32bit numbers to specify the size of the data that follows so this seems the cause of the server crash.

Another simple test is the modification of the 32bit values in the UDP query packets used to define the length of some strings.

- > *The multiplayer demo of this game*
- > *is subject to denial of service.*

Due the type of bug probably also the retail version is vulnerable.
Who bet?

BYEZ

Luigi Auriemma

<http://aluigi.altervista.org>