

# [NT] Race Driver Multiple Vulnerabilities (Broadcast Format String, Buffer-Overflow)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-07/0052.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 07/20/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 20 Jul 2005 16:49:20 +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>

-----  
Race Driver Multiple Vulnerabilities (Broadcast Format String,  
Buffer-Overflow)

---

## SUMMARY

<<http://www.codemasters.com>> Race Driver is "a racing game that allow the player to feel like a racing driver".

Lack of length and content checking allows attackers to cause the program to trigger inside the program a format string vulnerable and various buffer overflows, which in turn can be used to cause the Race Driver to execute arbitrary.

## DETAILS

Vulnerable Systems:

\* Race Driver version 1.20

Race Driver uses incorrectly the `sprintf()` function for building different types of text strings usually used for the visualization of the data. The places where this bad usage of `sprintf()` can be exploited are at least 2: the public chat hosted on the encrypted IRC server [peerchat.gamespy.com](http://peerchat.gamespy.com) and the in-game server browser.



=====  
=====

**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.