

# [NT] Judge Dredd Vs. Death Format String Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0009.html>

---

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

*Date:* 10/04/04

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

Date: 4 Oct 2004 14:02:36 +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>

-----

Judge Dredd Vs. Death Format String Vulnerability

---

## SUMMARY

Dredd vs Death is an FPS game based on the homonym comic strip. The game has been developed by <<http://www.rebellion.co.uk>> Rebellion and has been released in October 2003.

A format string vulnerability exists in the code that handles chat messages from connected clients.

## DETAILS

Vulnerable Systems:

\* Judge Dredd vs. Death at version 1.01 and prior

In order to demonstrate the problem it is only necessary to set up a server and a client. While the client is connected to the server, sending the following chat message will bring down the server immediately:

```
%n%n%n%n
```

Naturally a connected client requirement implies that an attacker has access to the server in question. Mechanisms such as passwords might

prevent this.

ADDITIONAL INFORMATION

The information has been provided by <mailto:aluigi@autistici.org> Luigi Auriemma.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

**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.