

[NT] Multiple vulnerabilities in Hired Team: Trial

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0041.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/16/04

To: list@securiteam.com

Date: 16 Nov 2004 17:27:21 +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>

Multiple vulnerabilities in Hired Team: Trial

SUMMARY

Hired Team is a nice FPS game developed by <<http://eng.nmg.ru>> New Media Generation, released at the end of the year 2000. It seems to be the only game based on the Shine engine (created by the same developers). Multiple vulnerabilities allow an attacker to crash both the game client and game server.

DETAILS

Vulnerable Systems:

* Hired Team Versions 2.0 / 2.200 and prior.

In-game format string vulnerability:

The game is affected by a format string bug in the game console. This allows an attacker to join a server (that doesn't have password support, so anyone can enter in it) and crash it or execute malicious code simply sending a message containing the formatted arguments (like the classical %n%n%n).

Proof of Concept Code:

Launch a server and a client, join the server and use the console by pressing the ~ key. Then type a format string: i.e: %n%n%n

Securiteam: [NT] Multiple vulnerabilities in Hired Team: Trial

The server will crash immediately. A more simple and fast test is the following: launch the game, select Console from the main menu and type %x. You will see a message like: Unknown command "1015c888"

Match interruption through malformed packet:

Each time a new player joins, the server assigns an UDP port to him (usually the sequential ports after the server's one, by default 29199). If the server receives a packet containing unexpected data to one of these data ports, the match will be interrupted immediately.

Proof of Concept Code:

Send a packet to the UDP port 29200 of the server (or 29220 if you are testing the demo, it is the data port usually assigned to the admin) containing any data you want, like hello, asdf or any other type of data.

Status and kick problems:

During the testing of this game/engine I found also that if a client uses the status command, the server crash immediately. The other strange thing is that any player can kick the others (admin included) without limits.

Proof of Concept Code:

When you (client) connect to the server, from the console type: status to crash the server or kick NAME where NAME is the name of the player you want to kick.

Vendor Status:

The vendor has not replied to emails. Probably the Shine engine and Hired Team: Trial are no longer supported.

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.