

[NEWS] Soldier Of Fortune II Format String (Through PunkBuster)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00067.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 20 Feb 2006 19:26:06 +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>

Soldier Of Fortune II Format String (Through PunkBuster)

SUMMARY

" <<http://www.punkbuster.com/>> PunkBuster Anti-Cheat software technology and services combat online cheating in some of the most popular games being played over the Internet today. "

A format string vulnerability in PunkBuster allows attackers to crash the Soldier of Fortune II game or execute arbitrary code.

DETAILS

Vulnerable Systems:

- * PB for server version 1.180 and prior

Immune Systems:

- * PB for server version 1.183

The PunkBuster server module supports the automatic kick and ban of the players who use invalid cvars, for example with values outside the range specified by the server.

When this situation occurs PB kicks the client abusing the game's

[NEWS] Soldier Of Fortune II Format String (Through PunkBuster)

functions (like a clientkick command).

The message sent to the client contains both the name of the monitored cvar and its value on the client, the resulted string is identified as "reason".

The problem is that naturally Soldier of Fortune II makes no checks on the "reason" parameter (watch trap_DropClient) which is passed by PB or by the server administrator for kicking a player, so the subsequent sprintf() call is vulnerable to a format string attack.

Normally there is no way to exploit this bug if you are not the server administrator (typing: clientkick 0 %n%n%n%n%n%n) but by using PunkBuster allows any player inside the server to crash or possibly take the control of the remote system.

Proof of Concept:

1. launch a client
2. join a server (naturally with PunkBuster enabled)
3. type /pb_cvarlist
4. choose one of the monitored cvars like "snaps" for example
5. type: /set CVAR %n%n%n%n%n%n%n
- example: /set snaps %n%n%n%n%n%n%n
6. the server will crash after some second during the kicking of the client

ADDITIONAL INFORMATION

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

The original article can be found at:

<<http://aluigi.altervista.org/adv/sof2pbfs-adv.txt>>

<http://aluigi.altervista.org/adv/sof2pbfs-adv.txt>

=====

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@xxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====

=====

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.