

# [NEWS] Buffer Overflow In Soldier Of Fortune II

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0100.html>

---

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

**Date:** 03/22/05

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

Date: 22 Mar 2005 19:08:52 +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>

-----

Buffer Overflow In Soldier Of Fortune II

---

## SUMMARY

<<http://www.ravensoft.com>> Soldier of Fortune II is a widely played FPS game released in May 2002.

The Soldier of Fortune II game server can be crashed by sending a big `cl_guid` value.

## DETAILS

Vulnerable Systems:

\* Soldier Of Fortune II Version 1.03 gold and lower.

Sending the server a request with a big `cl_guid` value can crash the game server.

Exploit Code:

An exploit code for this vulnerability can be found at:

<<http://aluigi.altervista.org/poc/sof2guidboom.zip>>

<http://aluigi.altervista.org/poc/sof2guidboom.zip>

Vendor Status:

The game is still "officially" unpatched from months so it can be declared

Securiteam: [NEWS] Buffer Overflow In Soldier Of Fortune II

no longer supported.

An unofficial work-around only for the Windows version can be found here:

<<http://aluigi.altervista.org/patches/sof2-103-guidfix.zip>>

<http://aluigi.altervista.org/patches/sof2-103-guidfix.zip>

The workaround checks the length of the cl\_guid value and reject clients that send a value bigger than 64 bytes (the max size of the cl\_guid buffer).

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](mailto:list-unsubscribe@securiteam.com)

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