

# [NT] Half-Life Remote Server and Client Crashes

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0052.html>

---

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

**Date:** 07/14/04

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

Date: 14 Jul 2004 11:24:07 +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>

-----

Half-Life Remote Server and Client Crashes

---

## SUMMARY

Half-Life is one of the most successful FPS (First Person Shooter) games in existence. Even though it dates back to 1998, Half-Life is still one of the most played games and with its various expansions and MODs is still being played by many people all around the world.

A bug has been found by Terry Henning (a.k.a. Soul Beaver) in both the server and client modules of Half-Life which can be used by a remote attacker to crash either and cause a denial of service condition.

## DETAILS

Vulnerable Systems:

- \* Half-Life version that dates prior to June 7th (Steam and non-Steam)

Immune Systems:

- \* Half-Life version after June 7th (Steam only)

The crashing of either the server or client is due to a malformed packet that is mishandled by the application. Each Half-Life packet is composed by the first 8 bytes used to track packets and to reassemble splitted data, but this second feature is the cause of the crash because the game

## Securiteam: [NT] Half-Life Remote Server and Client Crashes

doesn't correctly manage the empty splitted packets (so composed by the first 8 bytes only). The crash is the effect of the copying of data to a read-only part of memory (.reloc of swds.dll).

An example of the first bytes comprising such a malformed packet is:

```
"\xFE\xFF\xFF\x00\x00\x00"
```

A utility that can send malformed packets is available at

[<http://alugi.altervista.org/poc/hlboom.zip>](http://alugi.altervista.org/poc/hlboom.zip)

<http://alugi.altervista.org/poc/hlboom.zip>.

Patch Availability:

A patch for Steam users is available since June 7th. The last patch for un-Steamed Half-Life is 1.1.1.0 and is no longer supported.

### ADDITIONAL INFORMATION

The information has been provided by [<mailto:alugi@autistici.org>](mailto:alugi@autistici.org) Luigi Auriemma.

The original article can be found at:

[<http://alugi.altervista.org/adv/hlboom-adv.txt>](http://alugi.altervista.org/adv/hlboom-adv.txt)

<http://alugi.altervista.org/adv/hlboom-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@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.