

Advisory: Half-Life remote buffer overflow vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2001-09/0211.html>

From: Stanley G. Bubrouski (stan@ccs.neu.edu)

Date: 09/21/01

Date: Thu, 20 Sep 2001 20:53:51 -0400 (EDT)

From: "Stanley G. Bubrouski" <stan@ccs.neu.edu>

To: bugtraq@securityfocus.com

Subject: Advisory: Half-Life remote buffer overflow vulnerability

Message-ID: <Pine.GSO.4.21.0109202025370.2305-100000@denali.ccs.neu.edu>

Author: Stan Bubrouski (stan@ccs.neu.edu)

Date: September 20, 2001

Program: Half-Life

Versions Affected: 1.1.0.8 (September 19, 2001) and all previous versions

Severity: A Half-Life server can exploit buffer overflow in Client to execute arbitrary code on their machines.

Vendor: Valve Software (<http://www.valvesoftware.com>)

Vendor Contacted: September 18, 2001

Vendor Status: A fix will be included in the next update

Details: There is a buffer overflow in the console command "connect" on Windows Half-Life clients. The "connect" command is a command available in the client console which is used to connect to game servers when given a specific IP address and port. The format of the command is as follows:

```
/connect IP:port
```

By running the command with around 128 characters it is possible to overflow the buffer and execute arbitrary code. While this problem is on the client side it is still a serious issue, since servers have a function named "g_engfuncs.pfnClientCommand" which allows the server to force clients to execute whatever console command they want. This means that this overflow can be exploited remotely by means of this function. A server administrator could easily take advantage of this and exploit clients automatically as they connected to the server. An example of this would be Admin-Mod a popular remote administration plugin for many Half-Life mods like Counter-Strike, Team Fortress Classic, Day of Defeat, and Firearms. Admin-Mod has a command named admin_execclient which allows admins to force users to execute commands, including "connect."

Alfred Reynolds one of the maintainers of Admin-Mod was quick to point out to me that Admin-Mod's admin_execclient command only holds 100 characters

SecurityFocus Bugtraq: Advisory: Half-Life remote buffer overfl

and therefore would have to be modified to make use of this. He then also mentioned that since Admin-Mod is opensource anyone could modify the source and increase the buffer size anyways. Only part of one line of code in the Admin-Mod source would need to be changed to exploit this.

Of course this is not an issue with Admin-Mod I was just using it as an example.

Valve Software was contacted on September 18, 2001 and informed me it will be fixed in the next patch (presumably v1.1.0.9). They did not believe it to be a serious threat.

Solution: Install the patch when it becomes available.

Regards,

Stan

--

Stan Bubrowski
23 Westmoreland Road, Hingham, MA 02043

stan@ccs.neu.edu
Cell: (617) 835-3284

- **Previous message:** [Alexander Yurchenko: "Re: Local vulnerability in libutil derived with FreeBSD 4.4-RC \(and earlier\)"](#)
- **Next in thread:** [advisories@irmplc.com: "IRM Security Advisory: Xcache Path Disclosure Vulnerability"](#)
- **Reply:** [advisories@irmplc.com: "IRM Security Advisory: Xcache Path Disclosure Vulnerability"](#)
- **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)